L-9

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2000-305453**
(43)Date of publication of application : **02.11.2000**

(51)Int.Cl. G09C 1/00

(21)Application number : **11-114230**
(22)Date of filing : **21.04.1999**

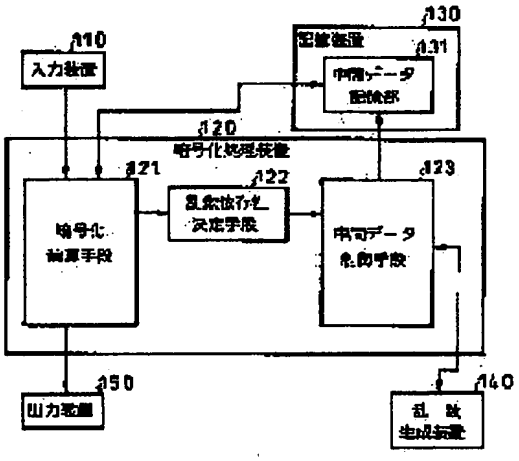
(71)Applicant : **NEC CORP**
(72)Inventor : **OBANA MASARU**

(54) CIPHERING DEVICE, DECIPHERING DEVICE, AND CIPHERING AND DECIPHERING DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a ciphering device, a deciphering device, and a ciphering and deciphering device having resistant property against deciphering analysis by means of measurement of electric power consumption such as electric power analysis and electric power differentiating analysis.

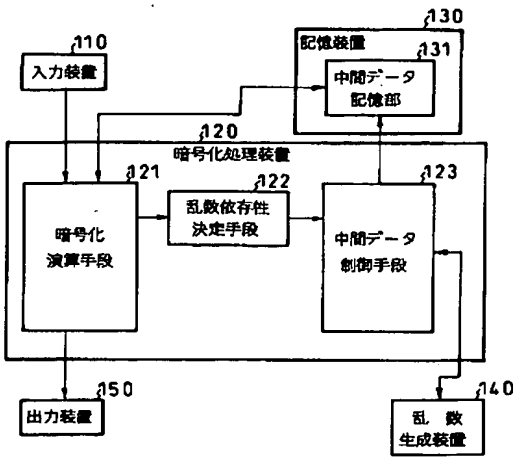
SOLUTION: An intermediate data control means 123, by using a random number outputted from a random number generator 140 as an input, executes a random number dependent intermediate data change operation to change intermediate data depending on the random number at the time of generation of an intermediate data change request, and controls to offset an effect of the random number by applying the random number dependent intermediate data change requests for a plurality of times. A ciphering operation means 121, by changing its state depending on the random number dependent intermediate data change operation, executes a ciphering process for usual sentences, outputs a ciphered sentence not depending on the random number. A random number dependent deciding means 122 issues the intermediate data change request when judging that the present processing stage of the ciphering process is the processing stage to apply the random number dependent intermediate data change operation.



L-9

閉じる

【発行国】日本国特許庁(JP)
【公報種別】公開特許公報
【公開番号】特開2000-305453(P2000-305453A)
【公開日】平成12年11月2日(2000.11.2)
【発明の名称】暗号化装置，復号装置，および暗号化・復号装置
【国際特許分類第7版】
IPC 識別 分冊
G09C 1/00 610
【FI】
FI 識別 分冊
G09C 1/00 610 A
【審査請求】有
【請求項の数】30
【出願形態】OL
【全頁数】28
【出願番号】特願平11-114230
【出願日】平成11年4月21日(1999.4.21)
【出願人】
000004237
日本電気株式会社
東京都港区芝五丁目7番1号
【発明者】
尾花 賢:
東京都港区芝五丁目7番1号 日本電気株式会社内
【代理人】
100088890
[弁理士]
河原 純一
【テーマコード(参考)】
5J104
【Fターム(参考)】
5J104 AA41 JA07 JA13 NA27 NA39



【要約】
【課題】 電力解析や電力差分解析等の消費電力の測定による暗号解析に対して耐性のある暗号化装置，復号装置，および暗号化・復号装置を提供する。
【解決手段】 中間データ制御手段123は、乱数生成装置140から出力される乱数を入力として、中間データを乱数に依存して変化させる乱数依存中間データ変更操作を中間データ変更要求の発生時点で行い、かつ当該乱数依存中間データ変更操作を複数回適用することによって乱数の効果を相殺するように制御する。
暗号化演算手段121は、乱数依存中間データ変更操作に依存して状態を変化させつつ、平文に対する暗号化処理を実行し、乱数に依存しない暗号文を出力する。
乱数依存性決定手段122は、暗号化処理の現在の処理段階が乱数依存中間データ変更操作を適用すべき処理段階であると判断した場合に、中間データ変更要求を発行する。
【特許請求の範囲】
【請求項1】 乱数を出力する乱数生成装置と、
前記乱数生成装置から出力される乱数を入力として、暗号化処理実行中に必要な中間データを乱数に依存して変化させる乱数依存中間データ変更操作を中間データ変更要求の発生時点で行い、かつ当該乱数依存中間データ変更操作を複数回適用することによって乱数の効果を相殺するように制御する中間データ制御手段と、
平文を入力とし、前記中間データ制御手段による乱数依存中間データ変更操作に依存して状態を変化させつつ当該平文に対する暗号化処理を実行し、当該平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力する暗号化演算手段と、
前記暗号化演算手段による暗号化処理の現在の処理段階が乱数依存中間データ変更操作を適用すべき処理段階であると判断した場合に、前記中間データ制御手段に対する中間データ変更要求を発行する乱数依存性決定手段とを備えたことを特徴とする暗号化装置。
【請求項2】 乱数を出力する乱数生成装置と、前記乱数生成装置から出力される乱数を入力として、暗号化処理手続きの実行順序を決定することや複数の処理手続きの選択肢の中から実際に実行される処理手続きを選択することを乱数に依存して行う乱数依存条件分岐決定操作を条件分岐決定要求の発生時点で行い、かつ暗号化演算手段の出力が乱数に依存しないように当該乱数依存条件分岐決定操作を制御する条件分岐制御手段と、
平文を入力とし、前記条件分岐制御手段による乱数依存条件分岐決定操作に依存して状態を変化させつつ当該平文に対する暗号化処理を実行し、当該平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力する暗号化演算手段と、
前記暗号化演算手段による暗号化処理の現在の処理段階が乱数依存条件分岐決定操作を適用すべき処理段階であると判断した場合に、前記条件分岐制御手段に対する条件分岐決定要求を発行する乱数依存性決定手段とを備えたことを特徴とする暗号化装置。
【請求項3】 乱数を出力する乱数生成装置と、
前記乱数生成装置から出力される乱数を入力として、暗号化処理中に意図的に挿入する実行遅延の遅延時間の決定を乱数に依存して行う乱数依存遅延挿入操作を遅延時間決定要求の発生時点で行う遅延制御手段と、
平文を入力とし、前記遅延制御手段による乱数依存遅延挿入操作に依存して状態を変化させつつ当該平文に対する暗号化処理を実行し、当該平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力する暗号化演算手段と、
前記暗号化演算手段による暗号化処理の処理段階が乱数依存遅延挿入操作を適用すべき処理段階であると判断した場合に、前記遅延制御手段に対する遅延時間決定要求を発行する乱数依存性決定手段とを備えたことを特徴とする暗号化装置。
【請求項4】 コンピュータシステムを、乱数を出力する乱数生成装置，前記乱数生成装置から出力される乱数を入力とし

て、暗号化処理実行中に必要な中間データを乱数に依存して変化させる乱数依存中間データ変更操作を中間データ変更要求の発生時点で行い、かつ当該乱数依存中間データ変更操作を複数回適用することによって乱数の効果を相殺するように制御する中間データ制御手段，平文を入力とし、前記中間データ制御手段による乱数依存中間データ変更操作に依存して状態を変化させつつ当該平文に対する暗号化処理を実行し、当該平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力する暗号化演算手段，および前記暗号化演算手段による暗号化処理の現在の処理段階が乱数依存中間データ変更操作を適用すべき処理段階であると判断した場合に、前記中間データ制御手段に対する中間データ変更要求を発行する乱数依存性決定手段として機能させるための暗号化処理プログラムを記録した記録媒体。

【請求項5】 コンピュータシステムを、乱数を出力する乱数生成装置，前記乱数生成装置から出力される乱数を入力として、暗号化処理手続きの実行順序を決定することや複数の処理手続きの選択肢の中から実際に実行される処理手続きを選択することを乱数に依存して行う乱数依存条件分岐決定操作を条件分岐決定要求の発生時点で行い、かつ暗号化演算手段の出力が乱数に依存しないように当該乱数依存条件分岐決定操作を制御する条件分岐制御手段，平文を入力とし、前記条件分岐制御手段による乱数依存条件分岐決定操作に依存して状態を変化させつつ当該平文に対する暗号化処理を実行し、当該平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力する暗号化演算手段，および前記暗号化演算手段による暗号化処理の現在の処理段階が乱数依存条件分岐決定操作を適用すべき処理段階であると判断した場合に、前記条件分岐制御手段に対する条件分岐決定要求を発行する乱数依存性決定手段として機能させるための暗号化処理プログラムを記録した記録媒体。

【請求項6】 コンピュータシステムを、乱数を出力する乱数生成装置，前記乱数生成装置から出力される乱数を入力として、暗号化処理中に意図的に挿入する実行遅延の遅延時間の決定を乱数に依存して行う乱数依存遅延挿入操作を遅延時間決定要求の発生時点で行う遅延制御手段，平文を入力とし、前記遅延制御手段による乱数依存遅延挿入操作に依存して状態を変化させつつ当該平文に対する暗号化処理を実行し、当該平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力する暗号化演算手段，および前記暗号化演算手段による暗号化処理の処理段階が乱数依存遅延挿入操作を適用すべき処理段階であると判断した場合に、前記遅延制御手段に対する遅延時間決定要求を発行する乱数依存性決定手段として機能させるための暗号化処理プログラムを記録した記録媒体。

【請求項7】 出力するデータが暗号化を行う平文そのものおよび平文に依存したデータのいずれかである乱数生成装置を備えたことを特徴とする請求項1，請求項2，または請求項3記載の暗号化装置。

【請求項8】 出力するデータが暗号化を行う平文そのものおよび平文に依存したデータのいずれかである乱数生成装置の機能を有する暗号化処理プログラムを記録したことを特徴とする請求項4，請求項5，または請求項6記載の記録媒体。

【請求項9】 乱数を出力する乱数生成装置と、
前記乱数生成装置から出力される乱数を入力として、復号処理実行中に必要な中間データを乱数に依存して変化させる乱数依存中間データ変更操作を中間データ変更要求の発生時点で行い、かつ当該乱数依存中間データ変更操作を複数回適用することによって乱数の効果を相殺するように制御する中間データ制御手段と、
暗号文を入力とし、前記中間データ制御手段による乱数依存中間データ変更操作に依存して状態を変化させつつ当該暗号文に対する復号処理を実行し、当該暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する復号演算手段と、
前記復号演算手段による復号処理の現在の処理段階が乱数依存中間データ変更操作を適用すべき処理段階であると判断した場合に、前記中間データ制御手段に対する中間データ変更要求を発行する乱数依存性決定手段とを備えたことを特徴とする復号装置。

【請求項10】 乱数を出力する乱数生成装置と、
前記乱数生成装置から出力される乱数を入力として、復号処理手続きの実行順序を決定することや複数の処理手続きの選択肢の中から実際に実行される処理手続きを選択することを乱数に依存して行う乱数依存条件分岐決定操作を条件分岐決定要求の発生時点で行い、かつ復号演算手段の出力が乱数に依存しないように当該乱数依存条件分岐決定操作を制御する条件分岐制御手段と、
暗号文を入力とし、前記条件分岐制御手段による乱数依存条件分岐決定操作に依存して状態を変化させつつ当該暗号文に対する復号処理を実行し、当該暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する復号演算手段と、
前記復号演算手段による復号処理の現在の処理段階が乱数依存条件分岐決定操作を適用すべき処理段階であると判断した場合に、前記条件分岐制御手段に対する条件分岐決定要求を発行する乱数依存性決定手段とを備えたことを特徴とする復号装置。

【請求項11】 乱数を出力する乱数生成装置と、
前記乱数生成装置から出力される乱数を入力として、復号処理中に意図的に挿入する実行遅延の遅延時間の決定を乱数に依存して行う乱数依存遅延挿入操作を遅延時間決定要求の発生時点で行う遅延制御手段と、
暗号文を入力とし、前記遅延制御手段による乱数依存遅延挿入操作に依存して状態を変化させつつ当該暗号文に対する復号処理を実行し、当該暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する復号演算手段と、
前記復号演算手段による復号処理の処理段階が乱数依存遅延挿入操作を適用すべき処理段階であると判断した場合に、前記遅延制御手段に対する遅延時間決定要求を発行する乱数依存性決定手段とを備えたことを特徴とする復号装置。

【請求項12】 コンピュータシステムを、乱数を出力する乱数生成装置，前記乱数生成装置から出力される乱数を入力として、復号処理実行中に必要な中間データを乱数に依存して変化させる乱数依存中間データ変更操作を中間データ変更要求の発生時点で行い、かつ当該乱数依存中間データ変更操作を複数回適用することによって乱数の効果を相殺するように制御する中間データ制御手段，暗号文を入力とし、前記中間データ制御手段による乱数依存中間データ変更操作に依存して状態を変化させつつ当該暗号文に対する復号処理を実行し、当該暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する復号演算手段，および前記復号演算手段による復号処理の現在の処理段階が乱数依存中間データ変更操作を適用すべき処理段階であると判断した場合に、前記中間データ制御手段に対する中間データ変更要求を発行する乱数依存性決定手段として機能させるための復号処理プログラムを記録した記録媒体。

【請求項13】 コンピュータシステムを、乱数を出力する乱数生成装置，前記乱数生成装置から出力される乱数を入力として、復号処理手続きの実行順序を決定することや複数の処理手続きの選択肢の中から実際に実行される処理手続きを選択することを乱数に依存して行う乱数依存条件分岐決定操作を条件分岐決定要求の発生時点で行い、かつ復号演算手段の出力が乱数に依存しないように当該乱数依存条件分岐決定操作を制御する条件分岐制御手段，暗号文を入力とし、前記条件分岐制御手段による乱数依存条件分岐決定操作に依存して状態を変化させつつ当該暗号文に対する復号処理を実行し、当該暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する復号演算手段，および前記復号演算手段による復号処理の現在の処理段階が乱数依存条件分岐決定操作を適用すべき処理段階であると判断した場合に、前記条件分岐制御手段に対する条件分岐決定要求を発行する乱数依存性決定手段として機能させるための復号処理プログラムを記録した記録媒体。

【請求項14】 コンピュータシステムを、乱数を出力する乱数生成装置，前記乱数生成装置から出力される乱数を入力として、復号処理中に意図的に挿入する実行遅延の遅延時間の決定を乱数に依存して行う乱数依存遅延挿入操作を遅延時間

決定要求の発生時点で行う遅延制御手段，暗号文を入力とし、前記遅延制御手段による乱数依存遅延挿入操作に依存して状態を変化させつつ当該暗号文に対する復号処理を実行し、当該暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する復号演算手段，および前記復号演算手段による復号処理の処理段階が乱数依存遅延挿入操作を適用すべき処理段階であると判断した場合に、前記遅延制御手段に対する遅延時間決定要求を発行する乱数依存性決定手段として機能させるための復号処理プログラムを記録した記録媒体。

【請求項15】　出力するデータが復号を行う暗号文そのものおよび暗号文に依存したデータのいずれかである乱数生成装置を備えたことを特徴とする請求項9，請求項10，または請求項11記載の復号装置。

【請求項16】　出力するデータが復号を行う暗号文そのものおよび暗号文に依存したデータのいずれかである乱数生成装置の機能を有する復号処理プログラムを記録したことを特徴とする請求項12，請求項13，または請求項14記載の記録媒体。

【請求項17】　乱数を出力する乱数生成装置と、
前記乱数生成装置から出力される乱数を入力として、暗号化処理実行中および復号処理実行中に必要な中間データを乱数に依存して変化させる乱数依存中間データ変更操作を中間データ変更要求の発生時点で行い、かつ当該乱数依存中間データ変更操作を複数回適用することによって乱数の効果を相殺するように制御する中間データ制御手段と、
処理データおよび処理内容を入力とし、前記中間データ制御手段による乱数依存中間データ変更操作に依存して状態を変化させつつ暗号化処理および復号処理を実行し、当該処理内容が暗号化処理であった場合には当該処理データである平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力し、当該処理内容が復号処理であった場合には当該処理データである暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する暗号化・復号演算手段と、
前記暗号化・復号演算手段による暗号化処理および復号処理の現在の処理段階が乱数依存中間データ変更操作を適用すべき処理段階であると判断した場合に、前記中間データ制御手段に対する中間データ変更要求を発行する乱数依存性決定手段とを備えたことを特徴とする暗号化・復号装置。

【請求項18】　乱数を出力する乱数生成装置と、
前記乱数生成装置から出力される乱数を入力として、暗号化処理手続きおよび復号処理手続きの実行順序を決定することや複数の処理手続きの選択肢の中から実際に実行される処理手続きを選択することを乱数に依存して行う乱数依存条件分岐決定操作を条件分岐決定要求の発生時点で行い、かつ暗号化・復号演算手段の出力が乱数に依存しないように当該乱数依存条件分岐決定操作を制御する条件分岐制御手段と、
処理データおよび処理内容を入力とし、前記条件分岐制御手段による乱数依存条件分岐決定操作に依存して状態を変化させつつ暗号化処理および復号処理を実行し、当該処理内容が暗号化処理であった場合には当該処理データである平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力し、当該処理内容が復号処理であった場合には当該処理データである暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する暗号化・復号演算手段と、
前記暗号化・復号演算手段による暗号化処理および復号処理の現在の処理段階が乱数依存条件分岐決定操作を適用すべき処理段階であると判断した場合に、前記条件分岐制御手段に対する条件分岐決定要求を発行する乱数依存性決定手段とを備えたことを特徴とする暗号化・復号装置。

【請求項19】　乱数を出力する乱数生成装置と、
前記乱数生成装置から出力される乱数を入力として、暗号化処理および復号処理中に意図的に挿入する実行遅延の遅延時間の決定を乱数に依存して行う乱数依存遅延挿入操作を遅延時間決定要求の発生時点で行う遅延制御手段と、
処理データおよび処理内容を入力とし、前記遅延制御手段による乱数依存遅延挿入操作に依存して状態を変化させつつ暗号化処理および復号処理を実行し、当該処理内容が暗号化処理であった場合には当該処理データである平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力し、当該処理内容が復号処理であった場合には当該処理データである暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する暗号化・復号演算手段と、
前記暗号化・復号演算手段による暗号化処理および復号処理の現在の処理段階が乱数依存遅延挿入操作を適用すべき処理段階であると判断した場合に、前記遅延制御手段に対する遅延時間決定要求を発行する乱数依存性決定手段とを備えたことを特徴とする暗号化・復号装置。

【請求項20】　コンピュータシステムを、乱数を出力する乱数生成装置，前記乱数生成装置から出力される乱数を入力として、暗号化処理実行中および復号処理実行中に必要な中間データを乱数に依存して変化させる乱数依存中間データ変更操作を中間データ変更要求の発生時点で行い、かつ当該乱数依存中間データ変更操作を複数回適用することによって乱数の効果を相殺するように制御する中間データ制御手段，処理データおよび処理内容を入力とし、前記中間データ制御手段による乱数依存中間データ変更操作に依存して状態を変化させつつ暗号化処理および復号処理を実行し、当該処理内容が暗号化処理であった場合には当該処理データである平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力し、当該処理内容が復号処理であった場合には当該処理データである暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する暗号化・復号演算手段，ならびに前記暗号化・復号演算手段による暗号化処理および復号処理の現在の処理段階が乱数依存中間データ変更操作を適用すべき処理段階であると判断した場合に、前記中間データ制御手段に対する中間データ変更要求を発行する乱数依存性決定手段として機能させるための暗号化・復号処理プログラムを記録した記録媒体。

【請求項21】　コンピュータシステムを、乱数を出力する乱数生成装置，前記乱数生成装置から出力される乱数を入力として、暗号化処理手続きおよび復号処理手続きの実行順序を決定することや複数の処理手続きの選択肢の中から実際に実行される処理手続きを選択することを乱数に依存して行う乱数依存条件分岐決定操作を条件分岐決定要求の発生時点で行い、かつ暗号化・復号演算手段の出力が乱数に依存しないように当該乱数依存条件分岐決定操作を制御する条件分岐制御手段，処理データおよび処理内容を入力とし、前記条件分岐制御手段による乱数依存条件分岐決定操作に依存して状態を変化させつつ暗号化処理および復号処理を実行し、当該処理内容が暗号化処理であった場合には当該処理データである平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力し、当該処理内容が復号処理であった場合には当該処理データである暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する暗号化・復号演算手段，ならびに前記暗号化・復号演算手段による暗号化処理および復号処理の現在の処理段階が乱数依存条件分岐決定操作を適用すべき処理段階であると判断した場合に、前記条件分岐制御手段に対する条件分岐決定要求を発行する乱数依存性決定手段として機能させるための暗号化・復号処理プログラムを記録した記録媒体。

【請求項22】　コンピュータシステムを、乱数を出力する乱数生成装置，前記乱数生成装置から出力される乱数を入力として、暗号化処理および復号処理中に意図的に挿入する実行遅延の遅延時間の決定を乱数に依存して行う乱数依存遅延挿入操作を遅延時間決定要求の発生時点で行う遅延制御手段，処理データおよび処理内容を入力とし、前記遅延制御手段による乱数依存遅延挿入操作に依存して状態を変化させつつ暗号化処理および復号処理を実行し、当該処理内容が暗号化処理であった場合には当該処理データである平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力し、当該処理内容が復号処理であった場合には当該処理データである暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する暗号化・復号演算手段，ならびに前記暗号化・復号演算手段による暗号化

処理および復号処理の現在の処理段階が乱数依存遅延挿入操作を適用すべき処理段階であると判断した場合に、前記遅延制御手段に対する遅延時間決定要求を発行する乱数依存性決定手段として機能させるための暗号化・復号処理プログラムを記録した記録媒体。
【請求項23】 暗号化処理の際に出力するデータが暗号化を行う平文そのものおよび平文に依存したデータのいずれかであり、復号処理の際に出力するデータが復号を行う暗号文そのものおよび暗号文に依存したデータのいずれかである乱数生成装置を備えたことを特徴とする請求項17，請求項18，または請求項19記載の暗号化・復号装置。
【請求項24】 暗号化処理の際に出力するデータが暗号化を行う平文そのものおよび平文に依存したデータのいずれかであり、復号処理の際に出力するデータが復号を行う暗号文そのものおよび暗号文に依存したデータのいずれかである乱数生成装置の機能を有する暗号化・復号処理プログラムを記録したことを特徴とする請求項20，請求項21，または請求項22記載の記録媒体。
【請求項25】 平文に加えて暗号化鍵を入力とする暗号化演算手段を備えることを特徴とする請求項1，請求項2，請求項3，または請求項7記載の暗号化装置。
【請求項26】 平文に加えて暗号化鍵を入力とする暗号化演算手段の機能を有する暗号化処理プログラムを記録したことを特徴とする請求項4，請求項5，請求項6，または請求項8記載の記録媒体。
【請求項27】 暗号文に加えて復号鍵を入力とする復号演算手段を備えることを特徴とする請求項9，請求項10，請求項11，または請求項15記載の復号装置。
【請求項28】 暗号文に加えて復号鍵を入力とする復号演算手段の機能を有する復号処理プログラムを記録したことを特徴とする請求項12，請求項13，請求項14，または請求項16記載の記録媒体。
【請求項29】 暗号化処理の際に処理データに加えて暗号化鍵を入力とし復号処理の際に処理データに加えて復号鍵を入力とする暗号化・復号演算手段を備えることを特徴とする請求項17，請求項18，請求項19，または請求項23記載の暗号化・復号装置。
【請求項30】 暗号化処理の際に処理データに加えて暗号化鍵を入力とし復号処理の際に処理データに加えて復号鍵を入力とする暗号化・復号演算手段の機能を有する暗号化・復号処理プログラムを記録したことを特徴とする請求項20，請求項21，請求項22，または請求項24記載の記録媒体。
【発明の詳細な説明】
【0001】
【発明の属する技術分野】 本発明は、暗号化鍵を用いて平文の暗号化を行い暗号文を生成する暗号化装置および復号鍵を用いて暗号文の復号を行い平文を生成する復号装置ならびに暗号化装置と復号装置との機能を併有する暗号化・復号装置に関する。
なお、暗号化装置と復号装置とは、それぞれの入力は異なるが構成や演算の内容は同様であるので、以下では主に暗号化装置で代表させて説明を行う。
【0002】
【従来の技術】 従来の暗号化装置は、入力装置と記憶装置と暗号化処理装置と出力装置とから構成されており、次のように動作する。
【0003】 すなわち、入力装置より暗号化処理装置に平文が入力され、平文を入力した暗号化処理装置は暗号化処理の中間段階で必要となる中間データを記憶装置に格納しつつ、常に予め定められた一定の処理順序に従って暗号化処理を行い、生成した暗号文を出力装置を通じて出力する。
このとき、暗号化処理の開始時から特定の暗号化中間処理手続きが開始されるまでに要する時間は、おおよそ一定になる。
【0004】 なお、暗号アルゴリズムの実装方法については、『「Applied Cryptography」(Bruce Shneier著) John Wiley & Sons, Inc. , 1996, ISBN 0−471−11709−9, pp. 623−673』に詳しく述べられている。
【0005】
【発明が解決しようとする課題】 上述した従来の技術による暗号化装置には、電力解析(シンプル・パワー・アナリシス)や電力差分解析(ディファレンシャル・パワー・アナリシス)と呼ばれる暗号解析法が有効であるという問題が存在する。
【0006】 電力解析および電力差分解析は、現在のメモリやレジスタ等の半導体デバイスにおいて、特定の時刻に当該半導体デバイスの保持する値に変化があった場合に、当該時刻における消費電力が保持する値に変化がなかった場合と比較して大きくなるという特徴を利用して、暗号化装置が平文の暗号化を行っている複数の時点で暗号化装置が消費する電力を測定することにより、暗号化装置が保持している秘密鍵(暗号化鍵)等の秘密情報を特定する暗号解析法である。
【0007】 電力解析や電力差分解析が有効に機能する条件としては、第1に消費電力を測定している各時点で行われている暗号化処理手続きが特定できること、第2に各時刻で測定した消費電力の値が当該時刻において暗号化装置内で行われている暗号化処理の演算結果を顕著に反映していること、の2点が挙げられる。
【0008】 従来の暗号化装置(復号装置および暗号化・復号装置も同様)においては、上記の2点の条件が満たされてしまうために、先に述べたように、電力解析や電力差分解析が有効に機能し、暗号の解読が可能になりうるという問題点が存在した。
【0009】 本発明の目的は、上述の点に鑑み、暗号化処理(復号処理も同様)の処理過程において乱数依存の状態変化を起こすことにより、消費電力を測定している各時点で行われている暗号化処理手続きを特定することを困難にすることで、電力解析および電力差分解析等の消費電力の測定による暗号解析に対して耐性のある暗号化装置(同様な復号装置および暗号化・復号装置を含む)を提供することにある。
【0010】 また、本発明の他の目的は、暗号化処理(復号処理も同様)の処理過程において乱数依存の状態変化を起こすことにより、各時刻で測定した消費電力の値と当該時刻に暗号化装置内で行われている暗号化処理との関連性を少なくすることで、電力解析および電力差分解析等の消費電力の測定による暗号解析に対して耐性のある暗号化装置(同様な復号装置および暗号化・復号装置を含む)を提供することにある。
【0011】 なお、本発明に対する従来技術に関する特許公報としては、特開平9−230786号公報および特開平8−504067号公報がある。
【0012】 上述の特開平9−230786号公報に記載された技術(データの暗号化方法及び装置)は、差分解読や線形解読を防止するための技術であり、暗号化の中間結果(本願発明における中間データ)を乱数には依存させずに変化させ、暗号化鍵を乱数に依存して変化させるものである。
【0013】 また、上述の特開平8−504067号公報に記載された技術(暗号化通信装置内の改善された機密性に関する方法および装置)は、電力遮断時等に、暗号化装置内の揮発性メモリに格納された鍵情報を能動的に消去し、電力供給再開時に同鍵情報をリロードするための技術である。
【0014】 これらの技術や当該両技術を組み合わせた技術では、最終的に出力される暗号文を乱数に依存しないようにすることは非常に困難である。
これに対して、本発明の暗号化装置は、乱数生成装置によって出力される乱数に依存しない暗号文を出力するという性質を持っている(乱数に依存するのは中間データのみで、最終的な出力である暗号文は乱数に依存しない)。
この点で、本発明は、上記の公報に記載された従来技術とは明確に異なっている。

【0015】
【課題を解決するための手段】本発明の暗号化装置は、乱数を出力する乱数生成装置と、前記乱数生成装置から出力される乱数を入力として、暗号化処理実行中に必要な中間データを乱数に依存して変化させる乱数依存中間データ変更操作を中間データ変更要求の発生時点で行い、かつ当該乱数依存中間データ変更操作を複数回適用することによって乱数の効果を相殺するように制御する中間データ制御手段と、平文を入力とし、前記中間データ制御手段による乱数依存中間データ変更操作に依存して状態を変化させつつ当該平文に対する暗号化処理を実行し、当該平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力する暗号化演算手段と、前記暗号化演算手段による暗号化処理の現在の処理段階が乱数依存中間データ変更操作を適用すべき処理段階であると判断した場合に、前記中間データ制御手段に対する中間データ変更要求を発行する乱数依存性決定手段とを有する。
【0016】また、本発明の暗号化装置は、乱数を出力する乱数生成装置と、前記乱数生成装置から出力される乱数を入力として、暗号化処理手続きの実行順序を決定することや複数の処理手続きの選択肢の中から実際に実行される処理手続きを選択することを乱数に依存して行う乱数依存条件分岐決定操作を条件分岐決定要求の発生時点で行い、かつ暗号化演算手段の出力が乱数に依存しないように当該乱数依存条件分岐決定操作を制御する条件分岐制御手段と、平文を入力とし、前記条件分岐制御手段による乱数依存条件分岐決定操作に依存して状態を変化させつつ当該平文に対する暗号化処理を実行し、当該平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力する暗号化演算手段と、前記暗号化演算手段による暗号化処理の現在の処理段階が乱数依存条件分岐決定操作を適用すべき処理段階であると判断した場合に、前記条件分岐制御手段に対する条件分岐決定要求を発行する乱数依存性決定手段とを有するように構成することも可能である。
【0017】さらに、本発明の暗号化装置は、乱数を出力する乱数生成装置と、前記乱数生成装置から出力される乱数を入力として、暗号化処理中に意図的に挿入する実行遅延の遅延時間の決定を乱数に依存して行う乱数依存遅延挿入操作を遅延時間決定要求の発生時点で行う遅延制御手段と、平文を入力とし、前記遅延制御手段による乱数依存遅延挿入操作に依存して状態を変化させつつ当該平文に対する暗号化処理を実行し、当該平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力する暗号化演算手段と、前記暗号化演算手段による暗号化処理の処理段階が乱数依存遅延挿入操作を適用すべき処理段階であると判断した場合に、前記遅延制御手段に対する遅延時間決定要求を発行する乱数依存性決定手段とを有するように構成することも可能である。
【0018】本発明の復号装置は、乱数を出力する乱数生成装置と、前記乱数生成装置から出力される乱数を入力として、復号処理実行中に必要な中間データを乱数に依存して変化させる乱数依存中間データ変更操作を中間データ変更要求の発生時点で行い、かつ当該乱数依存中間データ変更操作を複数回適用することによって乱数の効果を相殺するように制御する中間データ制御手段と、暗号文を入力とし、前記中間データ制御手段による乱数依存中間データ変更操作に依存して状態を変化させつつ当該暗号文に対する復号処理を実行し、当該暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する復号演算手段と、前記復号演算手段による復号処理の現在の処理段階が乱数依存中間データ変更操作を適用すべき処理段階であると判断した場合に、前記中間データ制御手段に対する中間データ変更要求を発行する乱数依存性決定手段とを有する。
【0019】また、本発明の復号装置は、乱数を出力する乱数生成装置と、前記乱数生成装置から出力される乱数を入力として、復号処理手続きの実行順序を決定することや複数の処理手続きの選択肢の中から実際に実行される処理手続きを選択することを乱数に依存して行う乱数依存条件分岐決定操作を条件分岐決定要求の発生時点で行い、かつ復号演算手段の出力が乱数に依存しないように当該乱数依存条件分岐決定操作を制御する条件分岐制御手段と、暗号文を入力とし、前記条件分岐制御手段による乱数依存条件分岐決定操作に依存して状態を変化させつつ当該暗号文に対する復号処理を実行し、当該暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する復号演算手段と、前記復号演算手段による復号処理の現在の処理段階が乱数依存条件分岐決定操作を適用すべき処理段階であると判断した場合に、前記条件分岐制御手段に対する条件分岐決定要求を発行する乱数依存性決定手段とを有するように構成することも可能である。
【0020】さらに、本発明の復号装置は、乱数を出力する乱数生成装置と、前記乱数生成装置から出力される乱数を入力として、復号処理中に意図的に挿入する実行遅延の遅延時間の決定を乱数に依存して行う乱数依存遅延挿入操作を遅延時間決定要求の発生時点で行う遅延制御手段と、暗号文を入力とし、前記遅延制御手段による乱数依存遅延挿入操作に依存して状態を変化させつつ当該暗号文に対する復号処理を実行し、当該暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する復号演算手段と、前記復号演算手段による復号処理の処理段階が乱数依存遅延挿入操作を適用すべき処理段階であると判断した場合に、前記遅延制御手段に対する遅延時間決定要求を発行する乱数依存性決定手段とを有するように構成することも可能である。
【0021】本発明の暗号化・復号装置は、乱数を出力する乱数生成装置と、前記乱数生成装置から出力される乱数を入力として、暗号化処理実行中および復号処理実行中に必要な中間データを乱数に依存して変化させる乱数依存中間データ変更操作を中間データ変更要求の発生時点で行い、かつ当該乱数依存中間データ変更操作を複数回適用することによって乱数の効果を相殺するように制御する中間データ制御手段と、処理データおよび処理内容を入力とし、前記中間データ制御手段による乱数依存中間データ変更操作に依存して状態を変化させつつ暗号化処理および復号処理を実行し、当該処理内容が暗号化処理であった場合には当該処理データである平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力し、当該処理内容が復号処理であった場合には当該処理データである暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する暗号化・復号演算手段と、前記暗号化・復号演算手段による暗号化処理および復号処理の現在の処理段階が乱数依存中間データ変更操作を適用すべき処理段階であると判断した場合に、前記中間データ制御手段に対する中間データ変更要求を発行する乱数依存性決定手段とを有する。
【0022】また、本発明の暗号化・復号装置は、乱数を出力する乱数生成装置と、前記乱数生成装置から出力される乱数を入力として、暗号化処理手続きおよび復号処理手続きの実行順序を決定することや複数の処理手続きの選択肢の中から実際に実行される処理手続きを選択することを乱数に依存して行う乱数依存条件分岐決定操作を条件分岐決定要求の発生時点で行い、かつ暗号化・復号演算手段の出力が乱数に依存しないように当該乱数依存条件分岐決定操作を制御する条件分岐制御手段と、処理データおよび処理内容を入力とし、前記条件分岐制御手段による乱数依存条件分岐決定操作に依存して状態を変化させつつ暗号化処理および復号処理を実行し、当該処理内容が暗号化処理であった場合には当該処理データである平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力し、当該処理内容が復号処理であった場合には当該処理データである暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する暗号化・復号演算手段と、前記暗号化・復号演算手段による暗号化処理および復号処理の現在の処理段階が乱数依存条件分岐決定操作を適用すべき処理段階であると判断した場合に、前記条件分岐制御手段に対する条件分岐決定要求を発行する乱数依存性決定手段とを有するように構成することも可能である。
【0023】さらに、本発明の暗号化・復号装置は、乱数を出力する乱数生成装置と、前記乱数生成装置から出力される乱数を入力として、暗号化処理および復号処理中に意図的に挿入する実行遅延の遅延時間の決定を乱数に依存して行う乱数依存遅延挿入操作を遅延時間決定要求の発生時点で行う遅延制御手段と、処理データおよび処理内容を入力とし、前記遅延制御手段による乱数依存遅延挿入操作に依存して状態を変化させつつ暗号化処理および復号処理を実行し、当該処理内容が暗号化処理であった場合には当該処理データである平文を暗号化した暗号文であって前記乱数生成装置の出力

に依存しない暗号文を出力し、当該処理内容が復号処理であった場合には当該処理データである暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する暗号化・復号演算手段と、前記暗号化・復号演算手段による暗号化処理および復号処理の現在の処理段階が乱数依存遅延挿入操作を適用すべき処理段階であると判断した場合に、前記遅延制御手段に対する遅延時間決定要求を発行する乱数依存性決定手段とを有するように構成することも可能である。

【0024】

【発明の実施の形態】 次に、本発明について図面を参照して詳細に説明する。

【0025】（1） 第1の実施の形態

図1は、本発明の第1の実施の形態に係る暗号化装置の構成を示すブロック図である。

【0026】本実施の形態に係る暗号化装置は、入力装置110と、暗号化処理装置120と、記憶装置130と、乱数生成装置140と、出力装置150とを含んで構成されている。

【0027】これらの装置は、それぞれ、概略次のように動作する。

【0028】入力装置110は、暗号化処理の対象となる平文を暗号化処理装置120に対して供給する。

【0029】暗号化処理装置120は、乱数生成装置140から出力される乱数と入力装置110より入力される平文とを入力として、当該平文を暗号化処理装置120内部に格納された鍵（暗号化鍵）で暗号化した暗号文を出力装置150から出力する。

【0030】ここで、暗号化処理装置120は、暗号化演算手段121と、乱数依存性決定手段122と、中間データ制御手段123とを備えている。

【0031】暗号化演算手段121は、入力装置110を通して供給される平文を入力とし、暗号化演算手段121に格納されている暗号化鍵を用いて当該平文の暗号化を行う。

暗号化演算手段121は、「中間データ制御手段123による中間データ（中間データ記憶部131に格納されているデータ）の乱数に依存した変更」を受けて状態を変化させつつ暗号化処理（複数の処理段階によって形成される暗号化処理）を実行し、最終的に当該平文を暗号化した暗号文を出力する。

なお、暗号化演算手段121は、暗号化処理実行中の複数の時点で、暗号化演算手段121による暗号化処理の現在の処理段階を乱数依存性決定手段122に送る（これにより、適切な処理段階で乱数に依存した状態の変化を生じさせることができる）。

【0032】乱数依存性決定手段122は、暗号化演算手段121が出力する暗号化演算手段121の現在の処理段階を入力として、当該処理段階に基づいて中間データ制御手段123に中間データ変更要求を出力すべきか否かを判断し、「中間データ変更要求の出力」を決定した場合（現在の処理段階が乱数に依存した操作を適用すべき処理段階であると判断した場合）には中間データ制御手段123に中間データ変更要求を出力する。

【0033】中間データ制御手段123は、乱数依存性決定手段122より出力される中間データ変更要求を入力した場合に、乱数生成装置140に乱数要求信号を送ることによって乱数を取得し、取得した乱数に依存して中間データ記憶部131に格納された中間データを変化させる操作（乱数依存中間データ変更操作）を行う。

【0034】なお、中間データ制御手段123は、乱数依存中間データ変更操作を複数回適用することによって、乱数の効果を相殺するように構成されている。

したがって、最終的に出力される暗号文は、乱数生成手段140から出力される乱数に依存しない。

【0035】記憶装置130は、中間データ記憶部131を備えている。

【0036】中間データ記憶部131は、暗号化処理装置120が行う暗号化処理中に保持する必要のある中間データを格納する。

なお、上記に示す通り、乱数依存性決定手段122から中間データ制御手段123に中間データ変更要求があった場合には、中間データ記憶部131に格納されている中間データは中間データ制御手段123によって操作される。

【0037】乱数生成装置140は、暗号化処理装置120より乱数要求信号を受け取り、当該乱数要求信号に基づいて暗号化処理装置120に乱数を出力する。

【0038】図2は、本実施の形態に係る暗号化装置の処理を示す流れ図である。

この処理は、平文入力ステップA1と、中間データ変更要求有無判定ステップA2と、乱数出力ステップA3と、乱数依存中間データ変更操作ステップA4と、暗号化処理一段階実行ステップA5と、暗号化処理終了判定ステップA6と、暗号文出力ステップA7とからなる。

【0039】次に、図1および 図2を参照して、本実施の形態に係る暗号化装置の全体の動作について詳細に説明する。

【0040】まず、暗号化を行いたい平文が、入力装置110から暗号化処理装置120内の暗号化演算手段121に入力される（ 図2のステップA1）。

【0041】暗号化演算手段121は、暗号化演算手段121による暗号化処理の現在の処理段階を乱数依存性決定手段122に出力する。

【0042】乱数依存性決定手段122は、暗号化演算手段121より受け取った暗号化演算手段121の処理段階に関する情報を基に、現在の処理段階が中間データ記憶部131に格納された中間データを乱数に依存して変更する処理段階であるか否かの判断を行い、「乱数に依存して中間データを変更する処理段階である」と判断した場合には中間データ制御手段123に中間データ変更要求を出力する。

【0043】中間データ制御手段123は、乱数依存性決定手段122からの中間データ変更要求があるか否かを判定する（ステップA2）。

【0044】中間データ制御手段123は、ステップA2で「中間データ変更要求がある」と判定した場合には、当該中間データ変更要求を受け取り、乱数要求（乱数要求信号）を乱数生成装置140に送り、当該乱数要求信号に基づいて乱数生成装置140から出力された乱数を得る（ステップA3）。

【0045】乱数を受け取った中間データ制御手段123は、記憶装置130内の中間データ記憶部131に格納されている中間データ（暗号化処理手段121が暗号化処理の中間段階において必要とするデータ）を受け取った乱数に依存して変更する乱数依存中間データ変更操作を行う（ステップA4）。

【0046】暗号化演算手段121は、ステップA4の乱数依存中間データ変更操作が終了した後に、またはステップA2で「中間データ変更要求がない」と判定した場合に、暗号化処理を一段階実行する（ステップA5）。

【0047】暗号化演算手段121は、暗号化処理を一段階実行したことで暗号化処理が終了したか否かを判定する（ステップA6）。

【0048】暗号化演算手段121は、ステップA6で「暗号化処理を一段階実行したことで暗号化処理が終了した」と判定した場合には、出力装置150に暗号文を出力し（ステップA7）、全体の処理を終了させる。

【0049】一方、暗号化演算手段121は、ステップA6で「暗号化処理が終了していない」と判定した場合（暗号化処理がまだ残されている場合）には、ステップA2に制御を戻して暗号化処理を継続させる。

【0050】次に、本実施の形態における効果について説明する。

【0051】本実施の形態では、暗号化処理の中間段階で必要なデータ（中間データ）が乱数に依存して変化しているために、中間データ間の演算を行っている時点の電力を測定することによって格納されている中間データの情報を引き出そうと

しても、中間データの値が乱数による影響を受けているために消費電力の変化が生じているのか、実際の暗号化処理に必要なデータの影響によって消費電力の変化が生じているのかを判断することが困難になる。
したがって、暗号化装置を電力解析や電力差分解析による暗号解析に対して耐性があるようにすることができる。
【0052】（2） 第2の実施の形態
図3は、本発明の第2の実施の形態に係る暗号化装置の構成を示すブロック図である。
【0053】図3を参照すると、本実施の形態に係る暗号化装置は、入力装置310と、暗号化処理装置320と、記憶装置330と、乱数生成装置340と、出力装置350とを含んで構成されている。
【0054】これらの装置は、それぞれ、概略次のように動作する。
【0055】入力装置310は、暗号化処理の対象となる平文を暗号化処理装置320に対して供給する。
【0056】暗号化処理装置320は、乱数生成装置340から出力される乱数と入力装置310より入力される平文とを入力として、当該平文を暗号化処理装置320の内部に格納された鍵（暗号化鍵）で暗号化した暗号文を出力装置350から出力する。
【0057】ここで、暗号化処理装置320は、暗号化演算手段321と、乱数依存性決定手段322と、条件分岐制御手段323とを備えている。
【0058】暗号化演算手段321は、入力装置310を通して供給される平文を入力とし、暗号化演算手段321に格納されている暗号化鍵を用いて当該平文の暗号化を行う。
暗号化演算手段321は、「条件分岐制御手段323による命令実行順序（暗号化処理手続きの実行順序）の決定および実行命令の選択（複数の処理手続きの選択肢の中から実際に実行される処理手続きを選択すること）の乱数に依存した変更」を受けて状態を変化させつつ暗号化処理（複数の処理段階によって形成される暗号化処理）を実行し、最終的に当該平文を暗号化した暗号文を出力する。
なお、暗号化演算手段321は、暗号化処理実行中の複数の時点で、暗号化演算手段321による暗号化処理の現在の処理段階を乱数依存性決定手段322に送る（これにより、適切な処理段階で乱数に依存した状態の変化を生じさせることができる）。
【0059】乱数依存性決定手段322は、暗号化演算手段321が出力する暗号化演算手段321の現在の処理段階を入力として、当該処理段階に基づいて条件分岐制御手段323に条件分岐決定要求を出力すべきか否かを判断し、「条件分岐決定要求の出力」を決定した場合（現在の処理段階が乱数に依存した操作を適用すべき処理段階であると判断した場合）には条件分岐制御手段324に条件分岐決定要求を出力する。
【0060】条件分岐制御手段323は、乱数依存性決定手段322より出力される条件分岐決定要求を入力した場合に、乱数生成装置340に乱数要求信号を送ることによって乱数を取得し、取得した乱数に依存して「実行順序を交換しても暗号化演算手段321の出力が変化しないような複数の暗号化処理手続きの実行順序の決定」および「どの処理手続きを実行しても暗号化演算手段321の出力が変化しないような複数の処理手続きの選択肢の中からの実行処理手続き（実際に実行する暗号化処理手続き）の選択」を行う操作（乱数依存条件分岐決定操作）を行う。
【0061】なお、条件分岐制御手段323は、前述のように暗号化演算手段321の出力が乱数に依存しないように乱数依存条件分岐決定操作を制御するように構成されている。
したがって、最終的に出力される暗号文は、乱数生成手段340から出力される乱数に依存しない。
【0062】記憶装置330は、中間データ記憶部331を備えている。
【0063】中間データ記憶部331は、暗号化処理装置320が行う暗号化処理中に保持する必要のある中間データを格納する。
【0064】乱数生成装置340は、暗号化処理装置320より乱数要求信号を受け取り、当該乱数要求信号に基づいて暗号化処理装置320に乱数を出力する。
【0065】図4は、本実施の形態に係る暗号化装置の処理を示す流れ図である。
この処理は、平文入力ステップB1と、条件分岐決定要求有無判定ステップB2と、乱数出力ステップB3と、乱数依存条件分岐決定操作ステップB4と、暗号化処理一段階実行ステップB5と、暗号化処理終了判定ステップB6と、暗号文出力ステップB7とからなる。
【0066】次に、図3および 図4を参照して、本実施の形態に係る暗号化装置の全体の動作について詳細に説明する。
【0067】まず、暗号化を行いたい平文が、入力装置310から暗号化処理装置320内の暗号化演算手段321に入力される（ 図4のステップB1）。
【0068】暗号化演算手段321は、暗号化演算手段321における暗号化処理の現在の処理段階を乱数依存性決定手段322に出力する。
【0069】乱数依存性決定手段322は、暗号化演算手段321より受け取った暗号化演算手段321の処理段階に関する情報を基に、現在の処理段階が乱数に依存した条件分岐の決定を行う処理段階であるか否かの判断を行い、「乱数に依存した条件分岐の決定を行う処理段階である」と判断した場合には条件分岐制御手段323に条件分岐決定要求を出力する。
【0070】条件分岐制御手段323は、乱数依存性決定手段322からの条件分岐決定要求があるか否かを判定する（ステップB2）。
【0071】条件分岐制御手段323は、ステップB2で「条件分岐決定要求がある」と判定した場合には、当該条件分岐決定要求を受け取り、乱数要求（乱数要求信号）を乱数生成装置340に送り、当該乱数要求信号に基づいて乱数生成装置340から出力された乱数を得る（ステップB3）。
【0072】乱数を受け取った条件分岐制御手段323は、受け取った乱数に依存して出力結果が同一となる複数の処理手続きの中から実際に行う処理手続きを選択等する乱数依存条件分岐決定操作を行う（ステップB4）。
【0073】暗号化演算手段321は、ステップB4の乱数依存条件分岐決定操作が終了した後に、またはステップB2で「条件分岐決定要求がない」と判定した場合には、暗号化処理を一段階実行する（ステップB5）。
【0074】暗号化演算手段321は、暗号化を一段階実行したことで暗号化処理が終了したか否かを判定する（ステップB6）。
【0075】暗号化演算手段321は、ステップB6で「暗号化を一段階実行したことで暗号化処理が終了した」と判定した場合には、出力装置350に暗号文を出力し（ステップB7）、全体の処理を終了させる。
【0076】一方、暗号化演算手段321は、ステップB6で「暗号化処理が終了していない」と判定した場合（暗号化処理がまだ残されている場合）には、ステップB2に制御を戻して暗号化処理を継続させる。
【0077】次に、本実施の形態における効果について説明する。
【0078】本実施の形態では、乱数によって実行される暗号化処理の順序や種類が変化するために、特定の時刻に着目しても当該時刻において暗号化処理装置320の内部で行われている処理が乱数によって異なっており、消費電力の変化を観測しても当該消費電力の変化がどの暗号化処理に対応しているのかを判断することが困難になる。
したがって、暗号化装置を電力解析や電力差分解析による暗号解析に対して耐性があるようにすることができる。
【0079】（3） 第3の実施の形態
図5は、本発明の第3の実施の形態に係る暗号化装置の構成を示すブロック図である。
【0080】図5を参照すると、本発明の実施の形態に係る暗号化装置は、入力装置510と、暗号化処理装置520と、記憶

装置530と、乱数生成装置540と、出力装置550とを含んで構成されている。
【0081】これらの装置は、それぞれ、概略次のように動作する。
【0082】入力装置510は、暗号化処理の対象となる平文を暗号化処理装置520に対して供給する。
【0083】暗号化処理装置520は、乱数生成装置540から出力される乱数と入力装置510より入力される平文とを入力として、当該平文を暗号化処理装置520の内部に格納された鍵(暗号化鍵)で暗号化した暗号文を出力装置550から出力する。
【0084】ここで、暗号化処理装置520は、暗号化演算手段521と、乱数依存性決定手段522と、遅延制御手段523とを備えている。
【0085】暗号化演算手段521は、入力装置510を通して供給される平文を入力とし、暗号化演算手段521に格納されている暗号化鍵を用いて当該平文の暗号化を行う。
暗号化演算手段521は、「遅延制御手段523による実行遅延時間の決定の乱数に依存した変更」を受けて状態を変化させつつ暗号化処理(複数の処理段階によって形成される暗号化処理)を実行し、最終的に当該平文を暗号化した暗号文を出力する。
なお、暗号化演算手段521は、暗号化処理実行中の複数の時点で、暗号化演算手段521による暗号化処理の現在の処理段階を乱数依存性決定手段522に送る(これにより、適切な処理段階で乱数に依存した状態の変化を生じさせることができる)。
【0086】乱数依存性決定手段522は、暗号化演算手段521が出力する暗号化演算手段521の現在の処理段階を入力として、当該処理段階に基づいて遅延制御手段523に遅延時間決定要求を出力すべきか否かを判断し、「遅延時間決定要求の出力」を決定した場合(現在の処理段階が乱数に依存した操作を適用すべき処理段階であると判断した場合)には遅延制御手段523に遅延時間決定要求を出力する。
【0087】遅延制御手段523は、乱数依存性決定手段522より出力される遅延時間決定要求を入力した場合に、乱数生成装置540に乱数要求信号を送ることによって乱数を取得し、取得した乱数に依存して暗号化処理中に意図的に発生させる実行遅延の遅延時間を決定して当該遅延を挿入する操作(乱数依存遅延挿入操作)を行う。
【0088】なお、遅延制御手段523は、暗号化演算手段521の処理に取得した乱数に応じた遅延を挿入する操作を行うように構成されており、遅延の挿入は暗号化に必要なデータにまったく乱数の影響をおよぼさない。
したがって、最終的に出力される暗号文は、乱数生成手段540から出力される乱数に依存しない。
【0089】記憶装置530は、中間データ記憶部531を備えている。
【0090】中間データ記憶部531は、暗号化処理装置520が行う暗号化処理中に保持する必要のある中間データを格納する。
【0091】乱数生成装置540は、暗号化処理装置520より乱数要求信号を受け取り、当該乱数要求信号に基づいて暗号化処理装置520に乱数を出力する。
【0092】図6は、本実施の形態に係る暗号化装置の処理を示す流れ図である。
この処理は、平文入力ステップC1と、遅延時間決定要求有無判定ステップC2と、乱数出力ステップC3と、乱数依存遅延挿入操作ステップC4と、暗号化処理一段階実行ステップC5と、暗号化処理終了判定ステップC6と、暗号文出力ステップC7とからなる。

【0093】次に、図5および 図6を参照して、本実施の形態に係る暗号化装置の全体の動作について詳細に説明する。
【0094】まず、暗号化を行いたい平文が、入力装置510から暗号化処理装置520内の暗号化演算手段521に入力される(図6のステップC1)。
【0095】暗号化演算手段521は、暗号化演算手段521における暗号化処理の現在の処理段階を乱数依存性決定手段522に出力する。
【0096】乱数依存性決定手段522は、暗号化演算手段521より受け取った暗号化演算手段521の処理段階に関する情報を基に、現在の処理段階が乱数に依存した遅延を挿入する処理段階(当該遅延の遅延時間を決定する処理段階)であるか否かの判断を行い、「乱数に依存した遅延を挿入する処理段階である」と判断した場合には遅延制御手段523に遅延時間決定要求を出力する。
【0097】遅延制御手段523は、乱数依存性決定手段522からの遅延時間決定要求があるか否かを判定する(ステップC2)。
【0098】遅延制御手段523は、ステップC2で「遅延時間決定要求がある」と判定した場合には、当該遅延時間決定要求を受け取り、乱数要求(乱数要求信号)を乱数生成装置540に送り、当該乱数要求信号に基づいて乱数生成装置540から出力された乱数を得る(ステップC3)。
【0099】乱数を受け取った遅延制御手段523は、受け取った乱数に依存して遅延時間を決定し、決定した遅延時間の実行遅延を暗号化処理中に意図的に挿入する(ステップC4)。
【0100】暗号化演算手段521は、ステップC4の乱数依存遅延挿入操作が終了した後に、またはステップB2で「乱数依存遅延時間決定要求がない」と判定した場合には、暗号化処理を一段階実行する(ステップC5)。
【0101】暗号化演算手段521は、暗号化を一段階実行したことで暗号化処理が終了したか否かを判定する(ステップC6)。
【0102】暗号化演算手段521は、ステップC6で「暗号化を一段階実行したことで暗号化処理が終了した」と判定した場合には、出力装置550に暗号文を出力し(ステップC7)、全体の処理を終了させる。
【0103】一方、暗号化演算手段521は、ステップC6で「暗号化処理が終了していない」と判定した場合(暗号化処理がまだ残されている場合)には、ステップC2に制御を戻して暗号化処理を継続させる。
【0104】次に、本実施の形態における効果について説明する。
【0105】本実施の形態では、乱数に依存した遅延時間の実行遅延が適宜挿入されるために、暗号解析に有用となる処理が行われている時刻が絶えず変化し、どの時刻の消費電力の変化に着目すれば効率的に暗号解析に必要な情報を得ることができるのかを特定することが困難になる。
したがって、暗号化装置を電力解析や電力差分解析による暗号解析に対して耐性があるようにすることができる。
【0106】なお、上述の第1, 第2, および第3の実施の形態に係る暗号化装置においては、暗号化鍵が予め暗号化演算手段(図1中の暗号化演算手段121, 図3中の暗号化演算手段321, および 図5中の暗号化演算手段521)に格納されていた。
【0107】しかし、入力装置(図1中の入力装置110, 図3中の入力装置310, および 図5中の入力装置510)から暗号化演算手段に暗号化鍵を入力するように、上記の暗号化装置を構成することも可能である。
この場合には、暗号化鍵を入力された暗号化演算手段は、その後に入力される1つまたは複数の平文の暗号化を当該暗号化鍵を用いて行い、暗号文を出力する。
【0108】上記のような構成を採用すると、暗号化鍵を外部から入力するようにできるため、暗号化演算手段自体を変更せずに暗号化鍵の更新を容易に行うことができるようになる。
【0109】また、上述の第1, 第2, および第3の実施の形態に係る暗号化装置においては、乱数生成装置(図1中の乱数

生成装置140，図3中の乱数生成装置340，および 図5中の乱数生成装置540）から出力される乱数を、入力装置から暗号化処理装置（図1中の暗号化処理装置120，図3中の暗号化処理装置320，および 図5中の暗号化処理装置520）に入力されるデータ（平文）そのものまたは当該データに依存したデータとすることも可能である。

【0110】このように平文を「乱数」として使用することが可能かつ有効になるのは、現在提案されている電力解析および電力差分解析では暗号文と消費電力とのみから暗号解析が行われており、平文のデータは暗号解析に使用されていないため、平文を乱数として利用することができるからである。

なお、乱数として「平文に依存したデータ」を用いるということは、例えば入力装置に入力される平文を暗号化鍵とは別の「乱数出力用鍵」で暗号化し、その暗号化の出力を乱数として利用するという暗号化装置も、本発明に含まれることになる。

【0111】（4） 第4の実施の形態

図7は、本発明の第4の実施の形態に係る暗号化装置の構成を示すブロック図である。

【0112】図7を参照すると、本発明の第4の実施の形態に係る暗号化装置は、図1に示した第1の実施の形態に係る暗号化装置に対して、暗号化処理プログラムを記録した記録媒体700を備える点が異なっている。

この記録媒体700は、磁気ディスク，半導体メモリ，CD－ROM（Compact Disk－ReadOnly Memory），その他の記録媒体であってよい。

【0113】暗号化処理プログラムは、記録媒体700からコンピュータシステム（入力装置110，暗号化処理装置120，記憶装置130，乱数生成装置140，および出力装置150を備えるコンピュータシステム）に読み込まれ、当該コンピュータシステムの動作を入力装置110，暗号化処理装置120（暗号化演算手段121，乱数依存性決定手段122，および中間データ制御手段123），記憶装置130（中間データ記憶部131），乱数生成装置140，および出力装置150として制御する。

暗号化処理プログラムの制御による入力装置110，暗号化処理装置120，記憶装置130，乱数生成装置140，および出力装置150の動作は、第1の実施の形態における入力装置110，暗号化処理装置120，記憶装置130，乱数生成装置140，および出力装置150の動作と全く同様になるので、その詳しい説明を割愛する。

【0114】（5） 第5の実施の形態

図8は、本発明の第5の実施の形態に係る暗号化装置の構成を示すブロック図である。

【0115】図8を参照すると、本発明の第5の実施の形態に係る暗号化装置は、図3に示した第2の実施の形態に係る暗号化装置に対して、暗号化処理プログラムを記録した記録媒体800を備える点が異なっている。

この記録媒体800は、磁気ディスク，半導体メモリ，CD－ROM，その他の記録媒体であってよい。

【0116】暗号化処理プログラムは、記録媒体800からコンピュータシステム（入力装置310，暗号化処理装置320，記憶装置330，乱数生成装置340，および出力装置350を備えるコンピュータシステム）に読み込まれ、当該コンピュータシステムの動作を入力装置310，暗号化処理装置320（暗号化演算手段321，乱数依存性決定手段322，および条件分岐制御手段323），記憶装置330（中間データ記憶部331），乱数生成装置340，および出力装置350として制御する。

暗号化処理プログラムの制御による入力装置310，暗号化処理装置320，記憶装置330，乱数生成装置340，および出力装置350の動作は、第2の実施の形態における入力装置310，暗号化処理装置320，記憶装置330，乱数生成装置340，および出力装置350の動作と全く同様になるので、その詳しい説明を割愛する。

【0117】（6） 第6の実施の形態

図9は、本発明の第6の実施の形態に係る暗号化装置の構成を示すブロック図である。

【0118】図9を参照すると、本発明の第6の実施の形態に係る暗号化装置は、図5に示した第3の実施の形態に係る暗号化装置に対して、暗号化処理プログラムを記録した記録媒体900を備える点が異なっている。

この記録媒体900は、磁気ディスク，半導体メモリ，CD－ROM，その他の記録媒体であってよい。

【0119】暗号化処理プログラムは、記録媒体900からコンピュータシステム（入力装置510，暗号化処理装置520，記憶装置530，乱数生成装置540，および出力装置550を備えるコンピュータシステム）に読み込まれ、当該コンピュータシステムの動作を入力装置510，暗号化処理装置520（暗号化演算手段521，乱数依存性決定手段522，および遅延制御手段523），記憶装置530（中間データ記憶部531），乱数生成装置540，および出力装置550として制御する。

暗号化処理プログラムの制御による入力装置510，暗号化処理装置520，記憶装置530，乱数生成装置540，および出力装置550の動作は、第3の実施の形態における入力装置510，暗号化処理装置520，記憶装置530，乱数生成装置540，および出力装置550の動作と全く同様になるので、その詳しい説明を割愛する。

【0120】（7） 第7の実施の形態

図10は、本発明の第7の実施の形態に係る復号装置の構成を示すブロック図である。

【0121】図10を参照すると、本実施の形態に係る復号装置は、入力装置1010と、復号演算手段1021，乱数依存性決定手段1022，および中間データ制御手段1023を備える復号処理装置1020と、中間データ記憶部1031を備える記憶装置1030と、乱数生成装置1040と、出力装置1050とを含んで構成されている。

【0122】本実施の形態に係る復号装置は、第1の実施の形態に係る暗号化装置と同様に、入力装置，復号処理装置（暗号化処理装置に該当する），記憶装置，乱数生成装置，および出力装置を備えている。

ここで、第1の実施の形態では、入力装置110からは平文が入力され、暗号化処理装置120が暗号化鍵を用いて平文の暗号化を行い、出力装置150から暗号文が出力されていた。

これに対し、本実施の形態では、入力装置1010からは暗号文が入力され、復号処理装置1020が復号鍵を用いて暗号文の復号を行い、出力装置1050から平文が出力される。

上記の点で、本実施の形態に係る復号装置は第1の実施の形態に係る暗号化装置と異なっている（それ以外の構成や動作は同様である）。

【0123】（8） 第8の実施の形態

図11は、本発明の第8の実施の形態に係る復号装置の構成を示すブロック図である。

【0124】図11を参照すると、本実施の形態に係る復号装置は、入力装置1110と、復号演算手段1121，乱数依存性決定手段1122，および条件分岐制御手段1123を備える復号処理装置1120と、中間データ記憶部1131を備える記憶装置1130と、乱数生成装置1140と、出力装置1150とを含んで構成されている。

【0125】本実施の形態に係る復号装置は、第2の実施の形態に係る暗号化装置と同様に、入力装置，復号処理装置（暗号化処理装置に該当する），記憶装置，乱数生成装置，および出力装置を備えている。

ここで、第2の実施の形態では、入力装置310からは平文が入力され、暗号化処理装置320が暗号化鍵を用いて平文の暗号化を行い、出力装置350から暗号文が出力されていた。

これに対し、本実施の形態では、入力装置1110からは暗号文が入力され、復号処理装置1120が復号鍵を用いて暗号文の復号を行い、出力装置1150から平文が出力される。

上記の点で、本実施の形態に係る復号装置は第2の実施の形態に係る暗号化装置と異なっている（それ以外の構成や動作は同様である）。

【0126】（9） 第9の実施の形態

図12は、本発明の第9の実施の形態に係る復号装置の構成を示すブロック図である。

【0127】図12を参照すると、本実施の形態に係る復号装置は、入力装置1210と、復号演算手段1221，乱数依存性決定手段1222，および遅延制御手段1223を備える復号処理装置1220と、中間データ記憶部1231を備える記憶装置12

30と、乱数生成装置1240と、出力装置1250とを含んで構成されている。
【0128】本実施の形態に係る復号装置は、第3の実施の形態に係る暗号化装置と同様に、入力装置，復号処理装置（暗号化処理装置に該当する），記憶装置，乱数生成装置，および出力装置を備えている。
ここで、第3の実施の形態では、入力装置510からは平文が入力され、暗号化処理装置520が暗号化鍵を用いて平文の暗号化を行い、出力装置550から暗号文が出力されていた。
これに対し、本実施の形態では、入力装置1210からは暗号文が入力され、復号処理装置1220が復号鍵を用いて暗号文の復号を行い、出力装置1250から平文が出力される。
上記の点で、本実施の形態に係る復号装置は第3の実施の形態に係る暗号化装置と異なっている（それ以外の構成や動作は同様である）。
【0129】なお、上述の第7，第8，および第9の実施の形態に係る復号装置においては、入力装置（ 図10中の入力装置1010，図11中の入力装置1110，および 図12中の入力装置1210）から復号演算手段（ 図10中の復号演算手段1021，図11中の復号演算手段1121，および 図12中の復号演算手段1221）に復号鍵を入力するように構成することも可能である。
【0130】また、上述の第7，第8，および第9の実施の形態に係る復号装置においては、乱数生成装置（図10中の乱数生成装置1040，図11中の乱数生成装置1140，および 図12中の乱数生成装置1240）から出力される乱数を、入力装置から復号処理装置（図10中の復号処理装置1020，図11中の復号処理装置1120，および 図12中の復号処理装置1220）に入力されるデータ（暗号文）そのものまたは当該データに依存したデータとすることも可能である。
【0131】（10） 第10の実施の形態
図13は、本発明の第10の実施の形態に係る復号装置の構成を示すブロック図である。
【0132】図13を参照すると、本発明の第10の実施の形態に係る復号装置は、図10に示した第7の実施の形態に係る復号装置に対して、復号処理プログラムを記録した記録媒体1300を備える点が異なっている。
この記録媒体1300は、磁気ディスク，半導体メモリ，CD－ROM，その他の記録媒体であってよい。
【0133】復号処理プログラムは、記録媒体1300からコンピュータシステム（入力装置1010，復号処理装置1020，記憶装置1030，乱数生成装置1040，および出力装置1050を備えるコンピュータシステム）に読み込まれ、当該コンピュータシステムの動作を入力装置1010，復号処理装置1020（復号演算手段1021，乱数依存性決定手段1022，および中間データ制御手段1023），記憶装置1030（中間データ記憶部1031），乱数生成装置1040，および出力装置1050として制御する。
復号処理プログラムの制御による入力装置1010，復号処理装置1020，記憶装置1030，乱数生成装置1040，および出力装置1050の動作は、第7の実施の形態における入力装置1010，復号処理装置1020，記憶装置1030，乱数生成装置1040，および出力装置1050の動作と全く同様になるので、その詳しい説明を割愛する。
【0134】（11） 第11の実施の形態
図14は、本発明の第11の実施の形態に係る復号装置の構成を示すブロック図である。
【0135】図14を参照すると、本発明の第11の実施の形態に係る復号装置は、図11に示した第8の実施の形態に係る復号装置に対して、復号処理プログラムを記録した記録媒体1400を備える点が異なっている。
この記録媒体1400は、磁気ディスク，半導体メモリ，CD－ROM，その他の記録媒体であってよい。
【0136】復号処理プログラムは、記録媒体1400からコンピュータシステム（入力装置1110，復号処理装置1120，記憶装置1130，乱数生成装置1140，および出力装置1150を備えるコンピュータシステム）に読み込まれ、当該コンピュータシステムの動作を入力装置1110，復号処理装置1120（復号演算手段1121，乱数依存性決定手段1122，および条件分岐制御手段1123），記憶装置1130（中間データ記憶部1131），乱数生成装置1140，および出力装置1150として制御する。
復号処理プログラムの制御による入力装置1110，復号処理装置1120，記憶装置1130，乱数生成装置1140，および出力装置1150の動作は、第8の実施の形態における入力装置1110，復号処理装置1120，記憶装置1130，乱数生成装置1140，および出力装置1150の動作と全く同様になるので、その詳しい説明を割愛する。
【0137】（12） 第12の実施の形態
図15は、本発明の第12の実施の形態に係る復号装置の構成を示すブロック図である。
【0138】図15を参照すると、本発明の第12の実施の形態に係る復号装置は、図12に示した第9の実施の形態に係る復号装置に対して、復号処理プログラムを記録した記録媒体1500を備える点が異なっている。
この記録媒体1500は、磁気ディスク，半導体メモリ，CD－ROM，その他の記録媒体であってよい。
【0139】復号処理プログラムは、記録媒体1500からコンピュータシステム（入力装置1210，復号処理装置1220，記憶装置1230，乱数生成装置1240，および出力装置1250を備えるコンピュータシステム）に読み込まれ、当該コンピュータシステムの動作を入力装置1210，復号処理装置1220（復号演算手段1221，乱数依存性決定手段1222，および遅延制御手段1223），記憶装置1230（中間データ記憶部1231），乱数生成装置1240，および出力装置1250として制御する。
復号処理プログラムの制御による入力装置1210，復号処理装置1220，記憶装置1230，乱数生成装置1240，および出力装置1250の動作は、第9の実施の形態における入力装置1210，復号処理装置1220，記憶装置1230，乱数生成装置1240，および出力装置1250の動作と全く同様になるので、その詳しい説明を割愛する。
【0140】（13） 第13の実施の形態
図16は、本発明の第13の実施の形態に係る暗号化・復号装置の構成を示すブロック図である。
【0141】図16を参照すると、本実施の形態に係る暗号化・復号装置は、入力装置1610と、暗号化・復号演算手段1621，乱数依存性決定手段1622，および中間データ制御手段1623を備える暗号化・復号処理装置1620と、中間データ記憶部1631を備える記憶装置1630と、乱数生成装置1640と、出力装置1650とを含んで構成されている。
【0142】本実施の形態に係る暗号化・復号装置は、第1の実施の形態に係る暗号化装置の機能と第7の実施の形態に係る復号装置の機能とを併有している。
ここで、入力装置1610，乱数依存性決定手段1622，中間データ制御手段1623，記憶装置1630，乱数生成装置1640，および出力装置1650は、第1の実施の形態や第7の実施における同名の構成要素と同様のものである。
【0143】暗号化・復号演算手段1621は、処理データおよび処理内容を入力とし、中間データ制御手段1623による乱数依存中間データ変更操作に依存して状態を変化させつつ暗号化処理および復号処理を実行し、当該処理内容が暗号化処理であった場合には当該処理データである平文を暗号化した暗号文であって乱数生成装置1640の出力に依存しない暗号文を出力し、当該処理内容が復号処理であった場合には当該処理データである暗号文を復号した平文であって乱数生成装置1640の出力に依存しない平文を出力する。
【0144】（14） 第14の実施の形態
図17は、本発明の第14の実施の形態に係る暗号化・復号装置の構成を示すブロック図である。
【0145】図17を参照すると、本実施の形態に係る暗号化・復号装置は、入力装置1710と、暗号化・復号演算手段1721，乱数依存性決定手段1722，および条件分岐制御手段1723を備える暗号化・復号処理装置1720と、中間データ記憶部1731を備える記憶装置1730と、乱数生成装置1740と、出力装置1750とを含んで構成されている。

【0146】本実施の形態に係る暗号化・復号装置は、第2の実施の形態に係る暗号化装置の機能と第8の実施の形態に係る復号装置の機能とを併有している。
ここで、入力装置1710，乱数依存性決定手段1722，条件分岐制御手段1723，記憶装置1730，乱数生成装置1740，および出力装置1750は、第2の実施の形態や第8の実施における同名の構成要素と同様のものである。
【0147】暗号化・復号演算手段1721は、処理データおよび処理内容を入力とし、条件分岐制御手段1723による乱数依存条件分岐決定操作に依存して状態を変化させつつ暗号化処理および復号処理を実行し、当該処理内容が暗号化処理であった場合には当該処理データである平文を暗号化した暗号文であって乱数生成装置1740の出力に依存しない暗号文を出力し、当該処理内容が復号処理であった場合には当該処理データである暗号文を復号した平文であって乱数生成装置1740の出力に依存しない平文を出力する。
【0148】（15） 第15の実施の形態
図18は、本発明の第15の実施の形態に係る暗号化・復号装置の構成を示すブロック図である。
【0149】図18を参照すると、本実施の形態に係る暗号化・復号装置は、入力装置1810と、暗号化・復号演算手段1821，乱数依存性決定手段1822，および遅延制御手段1823を備える暗号化・復号処理装置1820と、中間データ記憶部1831を備える記憶装置1830と、乱数生成装置1840と、出力装置1850とを含んで構成されている。
【0150】本実施の形態に係る暗号化・復号装置は、第3の実施の形態に係る暗号化装置の機能と第9の実施の形態に係る復号装置の機能とを併有している。
ここで、入力装置1810，乱数依存性決定手段1822，遅延制御手段1823，記憶装置1830，乱数生成装置1840，および出力装置1850は、第3の実施の形態や第9の実施における同名の構成要素と同様のものである。
【0151】暗号化・復号演算手段1821は、処理データおよび処理内容を入力とし、遅延制御手段1823による乱数依存遅延挿入操作に依存して状態を変化させつつ暗号化処理および復号処理を実行し、当該処理内容が暗号化処理であった場合には当該処理データである平文を暗号化した暗号文であって乱数生成装置1840の出力に依存しない暗号文を出力し、当該処理内容が復号処理であった場合には当該処理データである暗号文を復号した平文であって乱数生成装置1840の出力に依存しない平文を出力する。
【0152】なお、上述の第13，第14，および第15の実施の形態に係る暗号化・復号装置においては、入力装置（ 図16中の入力装置1610， 図17中の入力装置1710，および 図18中の入力装置1810）から暗号化・復号演算手段（ 図16中の暗号化・復号演算手段1621， 図17中の暗号化・復号演算手段1721，および 図18中の暗号化・復号演算手段1821）に暗号化鍵および復号鍵を入力するように構成することも可能である。
【0153】また、上述の第13，第14，および第15の実施の形態に係る暗号化・復号装置においては、乱数生成装置（ 図16中の乱数生成装置1640， 図17中の乱数生成装置1740，および 図18中の乱数生成装置1840）から出力される乱数を、入力装置から暗号化・復号処理装置（ 図16中の暗号化・復号処理装置1620， 図17中の暗号化・復号処理装置1720，および 図18中の暗号化・復号処理装置1820）に入力されるデータ（暗号文または平文）そのものまたは当該データに依存したデータとすることも可能である。
【0154】（16） 第16の実施の形態
図19は、本発明の第16の実施の形態に係る暗号化・復号装置の構成を示すブロック図である。
【0155】図19を参照すると、本発明の第16の実施の形態に係る暗号化・復号装置は、図16に示した第13の実施の形態に係る暗号化・復号装置に対して、暗号化・復号処理プログラムを記録した記録媒体1900を備える点が異なっている。この記録媒体1900は、磁気ディスク，半導体メモリ，CD－ROM，その他の記録媒体であってよい。
【0156】暗号化・復号処理プログラムは、記録媒体1900からコンピュータシステム（入力装置1610，暗号化・復号処理装置1620，記憶装置1630，乱数生成装置1640，および出力装置1650を備えるコンピュータシステム）に読み込まれ、当該コンピュータシステムの動作を入力装置1610，暗号化・復号処理装置1620（暗号化・復号演算手段1621，乱数依存性決定手段1622，および中間データ制御手段1623），記憶装置1630（中間データ記憶部1631），乱数生成装置1640，および出力装置1650として制御する。
暗号化・復号処理プログラムの制御による入力装置1610，暗号化・復号処理装置1620，記憶装置1630，乱数生成装置1640，および出力装置1650の動作は、第13の実施の形態における入力装置1610，暗号化・復号処理装置1620，記憶装置1630，乱数生成装置1640，および出力装置1650の動作と全く同様になるので、その詳しい説明を割愛する。
【0157】（17） 第17の実施の形態
図20は、本発明の第17の実施の形態に係る暗号化・復号装置の構成を示すブロック図である。
【0158】図20を参照すると、本発明の第17の実施の形態に係る暗号化・復号装置は、図17に示した第14の実施の形態に係る暗号化・復号装置に対して、暗号化・復号処理プログラムを記録した記録媒体2000を備える点が異なっている。この記録媒体2000は、磁気ディスク，半導体メモリ，CD－ROM，その他の記録媒体であってよい。
【0159】暗号化・復号処理プログラムは、記録媒体2000からコンピュータシステム（入力装置1710，暗号化・復号処理装置1720，記憶装置1730，乱数生成装置1740，および出力装置1750を備えるコンピュータシステム）に読み込まれ、当該コンピュータシステムの動作を入力装置1710，暗号化・復号処理装置1720（暗号化・復号演算手段1721，乱数依存性決定手段1722，および条件分岐制御手段1723），記憶装置1730（中間データ記憶部1731），乱数生成装置1740，および出力装置1750として制御する。
暗号化・復号処理プログラムの制御による入力装置1710，暗号化・復号処理装置1720，記憶装置1730，乱数生成装置1740，および出力装置1750の動作は、第14の実施の形態における入力装置1710，暗号化・復号処理装置1720，記憶装置1730，乱数生成装置1740，および出力装置1750の動作と全く同様になるので、その詳しい説明を割愛する。
【0160】（18） 第18の実施の形態
図21は、本発明の第18の実施の形態に係る暗号化・復号装置の構成を示すブロック図である。
【0161】図21を参照すると、本発明の第18の実施の形態に係る暗号化・復号装置は、図18に示した第15の実施の形態に係る暗号化・復号装置に対して、暗号化・復号処理プログラムを記録した記録媒体2100を備える点が異なっている。この記録媒体2100は、磁気ディスク，半導体メモリ，CD－ROM，その他の記録媒体であってよい。
【0162】暗号化・復号処理プログラムは、記録媒体2100からコンピュータシステム（入力装置1810，暗号化・復号処理装置1820，記憶装置1830，乱数生成装置1840，および出力装置1850を備えるコンピュータシステム）に読み込まれ、当該コンピュータシステムの動作を入力装置1810，暗号化・復号処理装置1820（暗号化・復号演算手段1821，乱数依存性決定手段1822，および遅延制御手段1823），記憶装置1830（中間データ記憶部1831），乱数生成装置1840，および出力装置1850として制御する。
暗号化・復号処理プログラムの制御による入力装置1810，暗号化・復号処理装置1820，記憶装置1830，乱数生成装置1840，および出力装置1850の動作は、第15の実施の形態における入力装置1810，暗号化・復号処理装置1820，記憶装置1830，乱数生成装置1840，および出力装置1850の動作と全く同様になるので、その詳しい説明を割愛する。
【0163】
【実施例】次に、本発明の実施例を、図面を参照して説明する。
【0164】（1） 第1の実施例
図22および 図23は、本発明の第1の実施例を説明するための図である。

【0165】本実施例は、上述の第1の実施の形態に係る暗号化装置を、共通鍵暗号DES(Data Encryption Standard)対応とするものである。
【0166】なお、DES暗号については、『「Handbook of AppliedCryptography」(A. Menezes, P. Oorschot, S. Vanstone著, CRC Press, 1997, ISBN 0−8493−8523−7)pp. 250−259』に詳しく述べられている。
【0167】ここでは、まず、図22を用いてDESの動作の概要を示す。
【0168】DESは、鍵スケジューリング部2210と、データ処理部2220とを備えている。
鍵スケジューリング部2210は、64ビットの暗号化鍵を入力とし、16個の48ビット中間鍵K_1 ～K_{16}を出力する。

データ処理部2220は、初期転置IPと、最終転置IP^{-1}と、16個のF関数とを備えており、64ビットの平文と鍵スケジューリング部2210から出力される16個の48ビットの中間鍵K_1 ～K_{16}を入力とし、64ビットの暗号文を出力する。

ここでIPおよびIP^{-1}は予め定められているビットの並び替えを行う関数であり、16個のF関数は32ビットのデータと48ビットのデータとを入力とし32ビットのデータを出力する予め定められた関数である。
【0169】平文の暗号化は次のように行われる。
【0170】まず、平文は、初期転置IPが施された後に、上位32ビットL_0と下位32ビットR_0とに分割される。

このL_0およびR_0から、次式に従ってL_1, R_1, L_2, R_2, L_3, R_3, …, L_{15}, R_{15}, L_{16}, R_{16}が生成される。
なお、上記のL_0, R_0, L_1, R_1, …が、図1中の中間データ記憶部131内の中間データに該当する。
【0171】
【数1】

$$L_n = R_{n-1}$$

$$R_n = L_{n-1} \oplus F(R_{n-1}, K_n) \quad \text{(但し } \oplus \text{ はビット毎の排他的論理和)}$$

【0172】ここで、n＝1, 2, …, 16である。
なお、上式の記号Fは、DESのF関数を表している。
【0173】DESの16個のF関数は、どれも同じ構造を持ち、32ビットのデータR_{n-1}と鍵スケジューリング部2210より出力される48ビットの中間鍵K_nとを入力とし、32ビットのデータを出力する。
上式を16回適用することによって得られたL_{16}を上位32ビットとし、R_{16}を下位32ビットとする64ビットのデータに対して最終転置IP^{-1}を施すことによって、64ビットの暗号文が得られる。
【0174】図23に、本実施例の概念を示す。
【0175】図23において破線で囲まれた部分(図23中の2310～2380)が、DESの暗号化の過程で必要になる中間データの変化に乱数依存性を持たせている部分(乱数依存性付与部分)である。
すなわち、当該乱数依存性付与部分が、図1中の中間データ制御手段123により行われる乱数依存中間データ変更操作を表している。
【0176】以下に、図22および 図23を基に、本実施例の構成および動作について説明する。
【0177】まず初めに、入力装置であるICカード・リーダ・ライタより平文が入力される。
平文は初期転置IPが施された後に、上位32ビットと下位32ビットとに分けられる。
この時点で中間データ制御手段が呼び出される。
中間データ制御手段は、乱数生成装置から2つの乱数r_0およびr_1を受け取り、上位32ビットのデータと乱数r_0との排他的論理和をとった結果をL_0に格納し(図23の2310参照)、下位32ビットのデータと乱数r_1との排他的論理和をとった結果をR_0に格納する(図23の2320参照)。
【0178】次に、n＝1, 2, …, 16に対し、以下の操作が繰り返される。
ただし、以下に現れるr*の値は次のように定義される。
【0179】
【数2】

$$r^* = \begin{cases} r_1 & (n = 1, 4, 7, 10, 13, 16 \text{ の時}) \\ r_0 \oplus r_1 & (n = 2, 5, 8, 11, 14 \text{ の時}) \\ r_0 & (n = 3, 6, 9, 12, 15 \text{ の時}) \end{cases}$$

【0180】まず、R_{n-1}の値がL_nに複写される。

続いて、再び中間データ制御手段が呼び出され、R_{n-1}とr*との排他的論理和がとられる(図23の2340, 2360, および2380参照)。
この排他的論理和の値とK_nとが、F関数への入力とされる。

以上の手続きにより、F関数への入力はR_{n-1}とK_nとなり、乱数生成装置から出力される乱数r*に依存していないことが確かめられる。
【0181】F関数の値が出力されると、中間データ制御手段が呼び出され、再びF関数の出力と乱数r*との排他的論理和がとられる(図23の2330, 2350, および2370参照)。
さらに、その結果とL_{n-1}との排他的論理和が計算され、計算結果がL_nに格納される。
【0182】上記操作を16回繰り返すことによって得られるL_{16}とr_1との排他的論理和をとった値を上位32ビットとし、R_{16}とr_0とr_1との排他的論理和をとった値を下位32ビットとする64ビットのデータに、最終転置IP^{-1}が施された64ビットのデータが、暗号文としてICカード・リーダ・ライタを通して出力される。
【0183】このとき得られる暗号文は、中間データを操作する乱数r_0およびr_1, 遅延時間を制御する乱数, ならびにS−boxの実行順序を決定する乱数のいずれの乱数にも依存しないデータになっている。
【0184】(2) 第2の実施例
図24, 図25, および 図26は、本発明の第2の実施例を説明するための図である。
【0185】本実施例は、上述の第2の実施の形態に係る暗号化装置を、共通鍵暗号RC5−32／12／16に適用したものである。
【0186】なお、RC5−32／12／16のアルゴリズムの詳細に関しては、上記の「Handbook of Applied Cryptography」のpp. 269−270に述べられている。
【0187】ここでは、まず、図24および 図25を参照して、RC5−32／12／16の動作を概説する。
【0188】RC5−32／12／16は、図24に示すように、128ビットの暗号化鍵2420を用いて64ビットの平文2410を64ビットの暗号文2450に変換するアルゴリズムである。
【0189】RC5−32／12／16は、データ処理部2430と、拡大鍵生成部2440とを有している。

【0190】拡大鍵生成部2440は、128ビットの暗号化鍵2420を入力とし、26個の32ビットの拡大鍵S_0, S_1, …, S_{25}を出力する。
【0191】データ処理部2430は、64ビットの平文2410と、拡大鍵生成部2440の出力S_0, S_1, …, S_{25}とを入力とし、64ビットの暗号文2450を出力する。
【0192】データ処理部2430は、次のように動作する。
【0193】まず、入力された64ビットの平文2410は、上位32ビットAと下位32ビットBとに分割される。
次に、AとS_0との2^{32}を法とする和(加算)がとられ、その結果が再びAに代入される(図24の2431参照)。
また、BとS_1との2^{32}を法とする和がとられ、その結果が再びBに代入される(図24の2432参照)。
その後、AおよびBは、ラウンド関数と呼ばれる変換を12回適用される。
【0194】暗号文2450は、ラウンド関数を12回適用した後のAを上位32ビットとして持ち、Bを下位32ビットとして持つ64ビットのデータとなる。
【0195】第i回目に適用されるラウンド関数は、A, B, S_{2i}, およびS_{2i+1}を入力としてAおよびBのデータの更新を行い、更新されたAおよびBを出力する。
【0196】次に、第i回目に適用されるラウンド関数の概要を説明する。
【0197】第i回目に適用されるラウンド関数によるAおよびBの更新は、次式に従って行われる。
【0198】
【数3】

$$A = ((A \oplus B) \lll B) + S_{2i}$$

$$B = ((B \oplus A) \lll A) + S_{2i+1}$$

【0199】ここで、「+」は2^{32}を法とする和を表し、「X<<<Y」はXのYビット回転を表している。
【0200】図25を参照すると、初めに、Aの更新が行われる。
まず、入力AはBとビット毎の排他的論理和2510をとられ、その結果がAに再び格納される。
次に、Aは、Bビットの左ビット回転2520を施され、その結果が再びAに格納される。
最後に、Aと拡大鍵S_{2i}との2^{32}を法とする和2530がとられ、その結果が更新後のAの値となる。
【0201】続いて、Bの更新が行われる。
まず、Bは、更新後のAとビット毎の排他的論理和2540をとられ、その結果がBに再び格納される。
次に、Bは、Aビットの左ビット回転2550を施され、その結果が再びBに格納される。
最後に、Bと拡大鍵S_{2i+1}との2^{32}を法とする和2560がとられ、その結果が更新後のBの値となる。
【0202】本実施例は、入力装置および出力装置としてICカード・リーダ・ライタを、データ記憶装置およびプログラムを格納した記憶媒体として半導体メモリを、暗号化処理装置としてICカードに内蔵されたコンピュータを備えている。
暗号化処理装置を実現するコンピュータは、汎用レジスタを5本以上有しており、また当該コンピュータの命令セットは、2つのレジスタR1, R2の算術和、ビット回転、ビット毎の排他的論理和等を計算した結果を必ずR1またはR2に格納するという特徴を有しているものとする。
ちなみに、現在使用されているコンピュータの多くは、上記のような特徴を持つ命令セットを有している。
【0203】次に、図26の流れ図と 図24および 図25とを基に、本実施例の全体的な動作について詳細に説明する。
【0204】図26の流れ図において、R1, R2, R3, R4およびR5はデータ幅32ビットの汎用レジスタを表しており、また表記「Ri←Ri+Rj」は汎用レジスタRiとRjとを加算した結果を新たに汎用レジスタRiに格納する操作を表している。
図26中の「Ri←Ri<<<Rj」等についても同様に解釈するものとする。
【0205】本実施例は、コンピュータが行う「Ri+Rj」および「Ri<<<Rj」等のレジスタ間演算の演算結果をRiおよびRjのどちらに格納するかを乱数に依存して変化させることを特徴としている。
【0206】演算結果の格納先を乱数に依存して変化させることで、電力を測定した場合の消費電力の変化が、汎用レジスタRiの値の変化によるものなのか、汎用レジスタRjの値の変化によるものなのかを検知することが困難になる。
【0207】次に、本実施例の動作の詳細な説明を行う。
【0208】本実施例では、まず初めに、入力装置を通じて暗号化処理装置に平文が格納される(図26のステップD1)。
【0209】平文が暗号化処理装置に入力されると、暗号化処理装置は汎用レジスタR1に加算(2^{32}を法とする和)2431が終了した後のAの値を格納し、汎用レジスタR3に加算(2^{32}を法とする和)2432が終了した後のBの値を格納する。
また、ラウンド関数の実行回数をカウントする変数rに1を格納する(ステップD2)。
【0210】次に、暗号化処理装置は、図25に示されるラウンド関数の2510および2520に対応する操作を実行し、さらに汎用レジスタR2にS_{2r}を格納する。
【0211】この時点で、条件分岐制御手段が呼び出され、R2の保持するS_{2r}の値とR1の保持するAの値との和(2^{32}を法とする和)2530をとった計算結果をR1およびR2のどちらに格納するかを乱数の値の偶奇数に応じて変化させる(ステップD3およびD4)。
【0212】図26のステップD4において乱数の値が奇数であった場合には、R2とR1との和の計算結果はR1に格納される。
引き続いて、暗号化演算手段はラウンド関数中の排他的論理和(ビット毎の排他的論理和)2540および左ビット回転2550を行い、左ビット回転2550が終了した時点におけるBの値をR3に格納する。
【0213】さらに、R4にS_{2r+1}の値を格納し、R3とR4との和をR3に格納する。
以上の操作により、ラウンド関数適用後のAおよびBの値がR1およびR3に格納される(ステップD5)。
【0214】ステップD5の処理が終了したことによって1回のラウンド関数の処理が終了する。
この時点で、現在までに暗号化処理装置が処理したラウンド関数の回数を表す変数rの値を調べ(ステップD7)、rの値がRC5−32／12／16が処理すべきラウンド関数の回数である12と等しかった場合には、出力装置から暗号文を出力して処理を終了する(ステップD9)。
それ以外の場合には、rに1を加え(ステップD8)、もう一度ラウンド関数を処理するためにステップD3に戻る。
【0215】ステップD4において乱数が偶数であった場合には、R2とR1との和の計算結果はR2に格納される。
【0216】引き続いて、暗号化処理装置はラウンド関数の排他的論理和(ビット毎の排他的論理和)2540および左ビット回転2550を行い、左ビット回転2550が終了した時点におけるBの値をR3に格納する。
【0217】さらに、R4にS_{2r+1}の値を格納し、R3とR4との和をR4に格納する。
以上の操作により、ラウンド関数適用後のAおよびBの値がR2およびR4に格納される(ステップD6)。
【0218】次に、ステップD7の場合と同様に変数rの値が12と等しいかどうかを調べ(ステップD14)、等しい場合には出力装置から暗号文を出力して処理を終了する(ステップD16)。
それ以外の場合には、rに1を加え(ステップD15)、もう一度ラウンド関数を処理するためにステップD10に進む。

【0219】ステップD10では、ラウンド関数への入力AおよびBの値がそれぞれR2およびR4に格納されている。
暗号化処理装置は、図25に示されるラウンド関数の排他的論理和2510および左ビット回転2520を実行し、さらに汎用レジスタR1にS_{2r}を格納する。

この時点で、条件分岐制御手段が呼び出され、R1の保持するS_{2r}の値とR2の保持するAの値との和(2^{32}を法とする和)2530をとった計算結果をR1およびR2のどちらに格納するかを乱数の値の偶奇に応じて変化させる(ステップD10およびD11)。
【0220】図26のステップD11において乱数の値が奇数であった場合には、R2とR1との和の計算結果はR1に格納される。
引き続いて、暗号化演算手段はラウンド関数中の排他的論理和2540および左ビット回転2550に対応する操作を行い、左ビット回転2550が終了した時点におけるBの値をR4に格納する。
さらにR3にS_{2r+1}の値を格納し、R3とR4との和をR3に格納する。

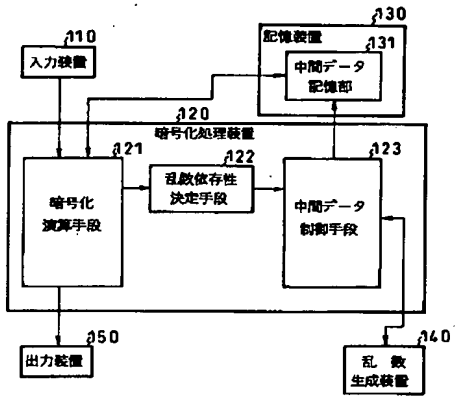
以上の操作により、ラウンド関数適用後のAおよびBの値がR1およびR3に格納される(ステップD12)。
【0221】ステップD12の処理が終了したことによって1回のラウンド関数の処理が終了する。
この時点で、現在までに暗号化処理装置が処理したラウンド関数の回数を表す変数rの値を調べ(ステップD7)、rの値がRC5−32／12／16が処理すべきラウンド関数の回数である12と等しかった場合には、出力装置から暗号文を出力して処理を終了する(ステップD9)。
それ以外の場合には、rに1を加え(ステップD8)、もう一度ラウンド関数を処理するためにステップD3に戻る。
【0222】ステップD11において乱数が偶数であった場合には、R2とR1との和の計算結果はR2に格納される。
引き続いて、暗号化処理装置はラウンド関数中の排他的論理和2540および左ビット回転2550に対応する操作を行い、左ビット回転2550が終了した時点におけるBの値をR4に格納する。
さらに、R3にS_{2r+1}の値を格納し、R3とR4との和をR4に格納する。

以上の操作により、ラウンド関数適用後のAおよびBの値がR2およびR4に格納される(ステップD13)。
【0223】次に、ステップD7の場合と同様に、変数rの値が12と等しいかどうかを調べ(ステップD14)、等しい場合には出力装置から暗号文を出力して処理を終了する(ステップD16)。
それ以外の場合には、rに1を加え(ステップD15)、もう一度ラウンド関数を処理するためにステップD10に戻る。
【0224】上記のアルゴリズムにより、乱数生成装置が出力した乱数の値に依存せずに、出力装置には入力平文を暗号化した結果が出力される。
【0225】(3) 第3の実施例
図27および 図28は、本発明の第3の実施例を説明するための図である。
【0226】本実施例は、上述の第15の実施の形態に係る暗号化・復号装置を、公開鍵暗号RSAに適用したものである。
【0227】なお、RSAのアルゴリズムに関しては、上記の「Handbook ofApplied Cryptography」のpp. 285−291に詳しく述べられている。
【0228】ここでは、まず、RSAの動作の概要を説明する。
【0229】RSAは512ビット程度の2つの素数p, qの積nと、lcm(p−1, q−1)(ただし、lcm(a, b)はaとbとの最小公倍数を表す)と互いに素である数eの組(n, e)とを公開鍵として持ち、法lcm(p−1, q−1)の下でed＝1となるようなdを秘密鍵として持つ。
【0230】RSAの暗号化は、次のように行われる。
【0231】Mを暗号化したい平文とすると、Mを暗号化した暗号文Cは次式に従って計算される。
【0232】$C=M^e \bmod n$
【0233】また、暗号文Cから平文Mを復号する計算は、次式で表される。
【0234】$M=C^d \bmod n$
【0235】RSAでは、暗号化や復号を高速に行うために、高速な冪乗剰余演算アルゴリズムが必要となる。
ここで冪乗剰余演算アルゴリズムとは、g, e, nを入力として$g^e \bmod n$を出力するアルゴリズムを指す。
【0236】RSAの実装では、高速な冪乗剰余演算アルゴリズムとして 図27の流れ図で示されるアルゴリズムまたはその改良アルゴリズムを用いることが標準的である。
ここでは、図27の流れ図を基に、高速冪乗剰余演算アルゴリズムの動作の流れを説明する。
【0237】冪乗剰余アルゴリズムでは、まず初めに、g, e, nが入力される(図27のステップE1)。
【0238】続いて、変数AおよびSに初期値として1およびgをそれぞれ格納する(ステップE2)。
【0239】続いて、eが0であるかどうかを判定し(ステップE3)、0の場合にはAを出力して処理を終了し、そうでない場合にはeの偶奇を調べ、eが奇数であった場合にはAとSとの積を計算し、その結果を新たに再びAに格納する(ステップE4およびE5)。
【0240】次に、eの値を2で割ることにより、eの1ビット右シフトを行う(ステップE6)。
【0241】この段階で再びeが0であるかどうかを判定し(ステップE7)、0である場合にはAを出力して処理を終了し、そうでない場合にはSを二乗して(ステップE8)、ステップE3に戻る。
【0242】eの二進数表現を$(b_1, b_2, \cdots, b_t)$とすると(ただし、b_1が最上位ビット、b_tが最下位ビット)、図27の流れ図においてステップE7をi回通過した時点でのAの値は、二進数表現が$(b_1, b_2, \cdots, b_i)$となるような数eiに対して$g^{ei} \bmod n$となっている。
【0243】アルゴリズムの構成法により、図27で示されるアルゴリズムではeのビット長tに対してアルゴリズム終了時までにステップE7を通過する回数は必ずt回となるので、アルゴリズム終了時のAの値は$g^e \bmod n$となり冪乗剰余演算が計算されていることが分かる。
【0244】しかし、上記のようなアルゴリズムを用いて冪乗剰余演算を実現する場合には、次のような問題が生じる。
図27のステップE4をi回通過した後にステップE5が実行される必要十分条件は、eの右からiビット目が1であることとなる。この時、上記のアルゴリズムを実装した装置の実行中に当該装置が消費する電力を測定することにより、当該装置内で実行されている命令の特定が可能であるとすると、RSA暗号文の復号時における当該装置の消費電力を測定することによりRSAの秘密鍵dを特定することが可能になってしまう。
【0245】次に、図27の流れ図および 図28を参照して本実施例を詳細に説明する。
【0246】本実施例の暗号化・復号装置における暗号化・復号処理装置2820は、暗号化・復号演算手段2821と、乱数依存性決定手段2822と、遅延制御手段2823とを備えており、次のように動作する。
【0247】暗号化・復号演算手段2821は、2つの相異なる数a, bと法nとを入力とし、$a \cdot b \bmod n$を計算する乗算器28211と、1つの数aと法nとを入力とし、$a^2 \bmod n$を計算する二乗演算器28212とを備えている。
【0248】暗号化・復号演算手段2821は、暗号化と復号との2つの機能を有しており、暗号化を行う場合には入力装置2810から通信相手の公開鍵e, n_1と送信したい平文Mとを入力し、図27の流れ図と同様な動作を行うことによって、暗号文

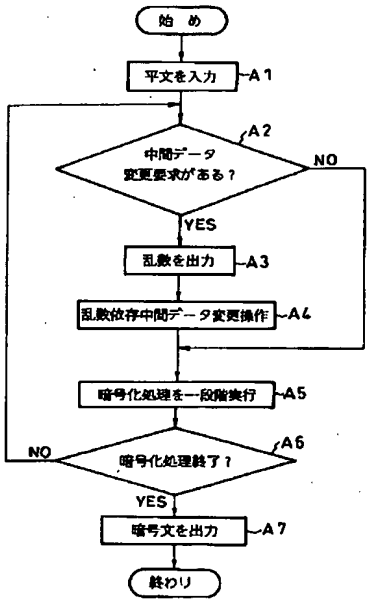
$M^e \bmod n_1$ を計算し、その計算結果を出力装置2850より出力する。
また、復号を行う場合には、入力装置2810から本人の秘密鍵dと本人の公開鍵n_2および受信した暗号文Cとを入力し、図27の流れ図と同様な動作を行うことによって、平文$C^d \bmod n_2$を計算し、その計算結果を出力装置2850より出力する。
【0249】図28中の暗号化・復号演算手段2821の動作が 図27の流れ図と異なる点は、図28中の暗号化・復号演算手段2821は、図27のステップE8からステップE3に戻る時点で乱数依存性決定手段2822によって遅延時間決定要求が遅延制御手段2823に出力される点にある。
【0250】遅延制御手段2823は、暗号化演算手段2821と同様に、乗算器28231と、二乗演算器28232とを備えており、乱数依存性決定手段2822より遅延時間決定要求が出されると、乱数生成装置2840に対して乱数要求信号を2度送り、2つの乱数r1, r2を得る。
【0251】r1とr2とを受け取った遅延制御手段2823は、r1の最下位ビットが0であるか否かを判定し、0であった場合には遅延挿入のために、二乗演算器28232を用いてr2の二乗の計算を行い、再び暗号化・復号演算手段2821に処理を移す。
一方、r1の最下位ビットが1であった場合には、遅延挿入のために、遅延制御手段2823は、乗算器28231を用いてr1とr2との積を計算した後に、二乗演算器28232を用いて乗算器28231の計算結果であるr1・r2の二乗を計算し、再び暗号化・復号演算手段2821に処理を移す。
【0252】
【発明の効果】以上説明したように、本発明の暗号化装置，復号装置，および暗号化・復号装置によると、データの暗号化や復号を行う際に当該装置の消費電力を測定することによって暗号化鍵や復号鍵等の秘密情報を得る暗号解析法（電力解析や電力差分解析等の消費電力の測定による暗号解析法）の適用が困難になるという効果が生じる。
【0253】以上のような効果が生じる理由を、以下に述べる。
【0254】電力解析や電力差分解析等の消費電力の測定による暗号解析が成功するためには、第1に暗号化装置や復号装置がデータの暗号化や復号を行っている際に消費する電力と当該装置内で行われている暗号化操作や復号操作との間に密接な関連があること、第2に暗号化装置や復号装置が特定の暗号化操作や復号操作を行っている時刻が容易に検知できること、の2点が必要条件となる。
【0255】本発明では、中間データ制御手段によって暗号化や復号を行う際に必要となる中間データが乱数に依存して変化したまま暗号装置や復号装置内で暗号化操作や復号操作が行われるため、当該装置が消費した電力の変化が実際の暗号化操作や復号操作によって生じたものであるのか、乱数の影響によって生じたものであるのかの判断が困難になっている。
したがって、暗号化装置や復号装置の消費電力と当該装置内で行われている暗号化操作や復号操作との間の関連が検知しづらくなるため、電力解析や電力差分解析が成功するための第1の必要条件が成立しなくなる。
【0256】さらに、本発明では、条件分岐制御手段によって、順序を入れ替えることが可能であるような操作の順序（実行順序）の決定や、どの操作を実行しても暗号化や復号の結果が変化しないような複数の操作の選択肢の中から実際に実行される操作を選択することを、乱数に依存して行っている。
また、遅延制御手段によって、暗号化や復号の操作の途中で、適宜乱数に依存した時間の遅延が挿入される。
それらのために、特定の暗号化や復号の操作が実行される時刻が、乱数によって変化することになる。
したがって、電力解析や電力差分解析が成功するための第2の必要条件が成立しなくなる。
【0257】以上により、電力解析や電力差分解析の成功に必要な2つの条件が成立しなくなるため、暗号化装置や復号装置の消費電力を測定することで秘密情報を得るという暗号解析法が困難になる。
【図面の簡単な説明】
【図1】本発明の第1の実施の形態に係る暗号化装置の構成を示すブロック図である。
【図2】図1に示す暗号化装置の処理を示す流れ図である。
【図3】本発明の第2の実施の形態に係る暗号化装置の構成を示すブロック図である。
【図4】図3に示す暗号化装置の処理を示す流れ図である。
【図5】本発明の第3の実施の形態に係る暗号化装置の構成を示すブロック図である。
【図6】図5に示す暗号化装置の処理を示す流れ図である。
【図7】本発明の第4の実施の形態に係る暗号化装置の構成を示すブロック図である。
【図8】本発明の第5の実施の形態に係る暗号化装置の構成を示すブロック図である。
【図9】本発明の第6の実施の形態に係る暗号化装置の構成を示すブロック図である。
【図10】本発明の第7の実施の形態に係る復号装置の構成を示すブロック図である。
【図11】本発明の第8の実施の形態に係る復号装置の構成を示すブロック図である。
【図12】本発明の第9の実施の形態に係る復号装置の構成を示すブロック図である。
【図13】本発明の第10の実施の形態に係る復号装置の構成を示すブロック図である。
【図14】本発明の第11の実施の形態に係る復号装置の構成を示すブロック図である。
【図15】本発明の第12の実施の形態に係る復号装置の構成を示すブロック図である。
【図16】本発明の第13の実施の形態に係る暗号化・復号装置の構成を示すブロック図である。
【図17】本発明の第14の実施の形態に係る暗号化・復号装置の構成を示すブロック図である。
【図18】本発明の第15の実施の形態に係る暗号化・復号装置の構成を示すブロック図である。
【図19】本発明の第16の実施の形態に係る暗号化・復号装置の構成を示すブロック図である。
【図20】本発明の第17の実施の形態に係る暗号化・復号装置の構成を示すブロック図である。
【図21】本発明の第18の実施の形態に係る暗号化・復号装置の構成を示すブロック図である。
【図22】本発明の第1の実施例を説明するための図（DESの構成を示すブロック図）である。
【図23】本発明の第1の実施例を説明するための図（当該実施例の構成を示すブロック図）である。
【図24】本発明の第2の実施例を説明するための図（RC5－32/12/16の構成を示すブロック図）である。
【図25】本発明の第2の実施例を説明するための図（RC5－32/12/16のラウンド関数の構成を示すブロック図）である。
【図26】本発明の第2の実施例を説明するための図（当該実施例の動作を示す流れ図）である。
【図27】本発明の第3の実施例を説明するための図（高速冪乗剰余演算の動作を示す流れ図）である。
【図28】本発明の第3の実施例を説明するための図（当該実施例の構成を示すブロック図）である。
【符号の説明】110, 310, 510, 1010, 1110, 1210, 1610, 1710, 1810, 2810 入力装置
120, 320, 520 暗号化処理装置
121, 321, 521 暗号化演算手段
122, 322, 522, 1022, 1122, 1222, 1622, 1722, 1822, 2822 乱数依存性決定手段
123, 1023, 1623 中間データ制御手段
130, 330, 530, 1030, 1130, 1230, 1630, 1730, 1830, 2830 記憶装置

131, 331, 531, 1031, 1131, 1231, 1631, 1731, 1831, 2831 中間データ記憶部
140, 340, 540, 1040, 1140, 1240, 1640, 1740, 1840, 2840 乱数生成装置
150, 350, 550, 1050, 1150, 1250, 1650, 1750, 1850, 2850 出力装置
323, 1123, 1723 条件分岐制御手段
523, 1223, 1823, 2823 遅延制御手段
700, 800, 900, 1300, 1400, 1500, 1900, 2000, 2100 記録媒体
1020, 1120, 1220 復号処理装置
1021, 1121, 1221 復号演算手段
1620, 1720, 1820, 2820 暗号化・復号処理装置
1621, 1721, 1821, 2821 暗号化・復号演算手段
2210 鍵スケジューリング部
2220, 2430 データ処理部
2310, 2320, 2330, 2340, 2350, 2360, 2370, 2380 乱数依存性付与部分
2410 平文
2420 暗号化鍵
2431, 2432, 2530, 2560 2^{32}を法とする和
2440 拡大鍵生成部
2450 暗号文
2510, 2540 ビット毎の排他的論理和
2520, 2550 左ビット回転
28211, 28231 乗算器
28212, 28232 二乗演算器

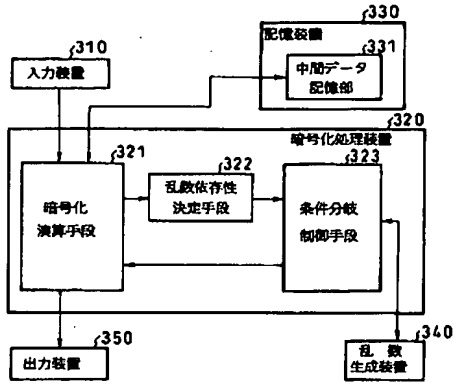
【図1】



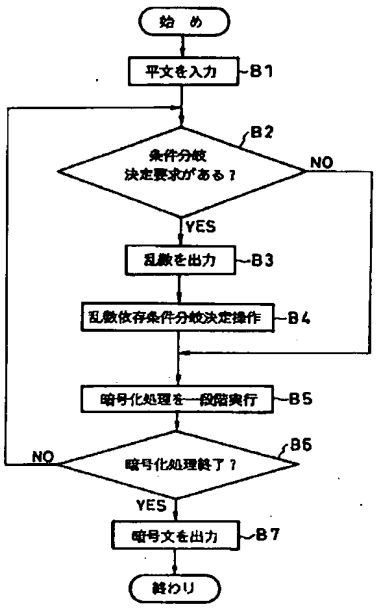
【図2】



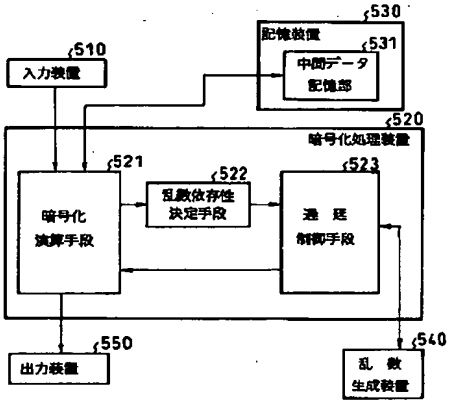
【図3】


330
記憶装置
331
中間データ
記憶部
310
入力装置
320
暗号化処理装置
321
暗号化
演算手段
322
乱数依存性
決定手段
323
条件分岐
制御手段
350
出力装置
340
乱 数
生成装置

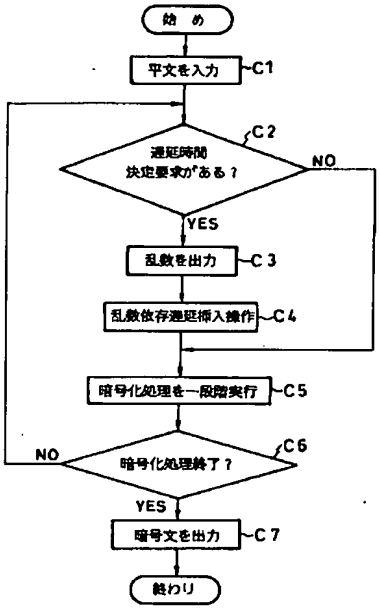
【図4】


始 め
平文を入力
B1
B2
条件分岐
決定要求がある？
NO
YES
乱数を出力
B3
乱数依存条件分岐決定操作
B4
暗号化処理を一段階実行
B5
B6
NO
暗号化処理終了？
YES
暗号文を出力
B7
終わり

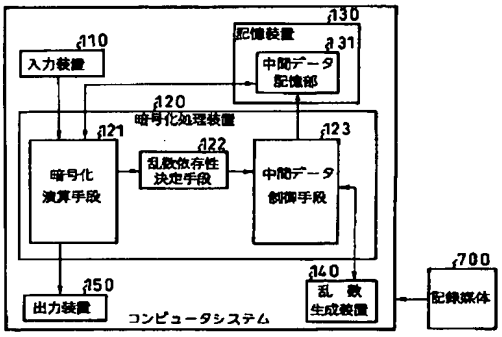
【図5】


530
記憶装置
531
中間データ
記憶部
510
入力装置
520
暗号化処理装置
521
暗号化
演算手段
522
乱数依存性
決定手段
523
遅 延
制御手段
550
出力装置
540
乱 数
生成装置

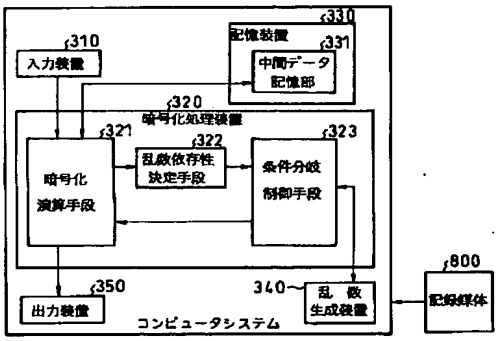
【図6】


始め
平文を入力
C1
遅延時間
決定要求がある？
C2
NO
YES
乱数を出力
C3
乱数依存遅延挿入操作
C4
暗号化処理を一段階実行
C5
暗号化処理終了？
C6
NO
YES
暗号文を出力
C7
終わり

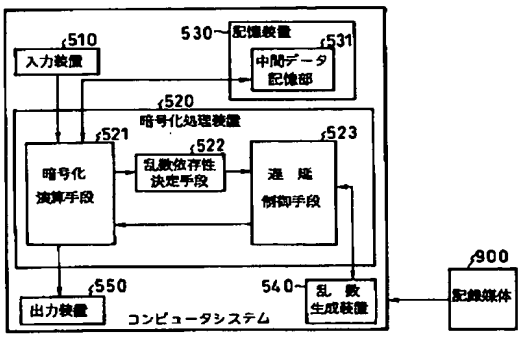
【図7】


110
入力装置
130
記憶装置
131
中間データ記憶部
120
暗号化処理装置
121
暗号化演算手段
122
乱数依存性決定手段
123
中間データ制御手段
150
出力装置
140
乱数生成装置
700
記録媒体
コンピュータシステム

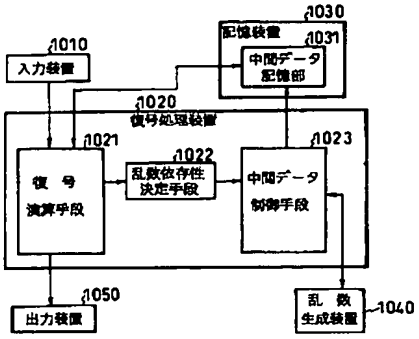
【図8】


310
入力装置
330
記憶装置
331
中間データ記憶部
320
暗号化処理装置
321
暗号化演算手段
322
乱数依存性決定手段
323
条件分岐制御手段
350
出力装置
340
乱数生成装置
800
記録媒体
コンピュータシステム

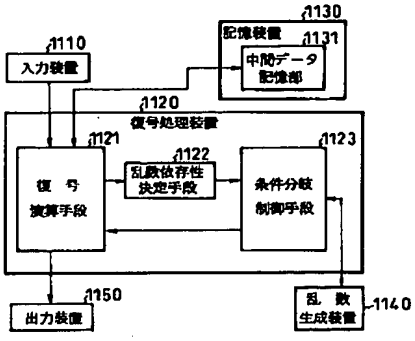
【図9】


510
入力装置
530
記憶装置
531
中間データ記憶部
520
暗号化処理装置
521
暗号化演算手段
522
乱数依存性決定手段
523
遅延制御手段
550
出力装置
540
乱数生成装置
900
記録媒体
コンピュータシステム

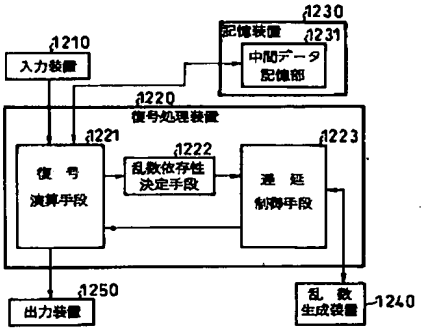
【図10】



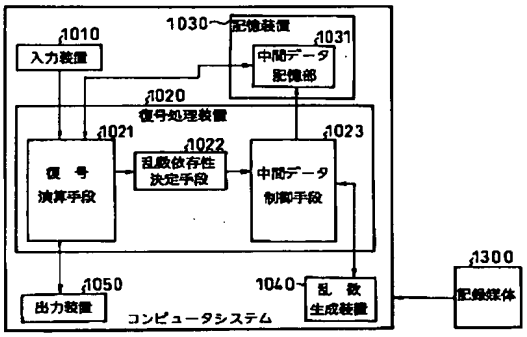
【図11】



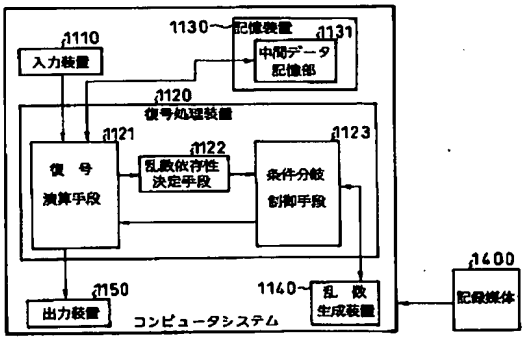
【図12】



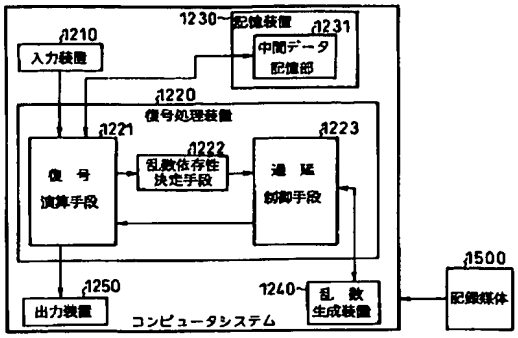
【図13】



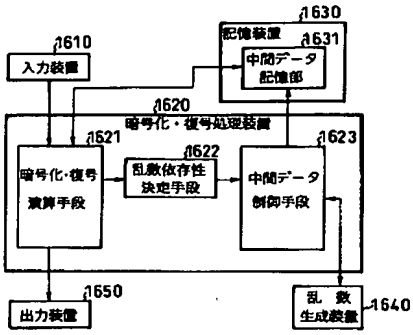
【図14】



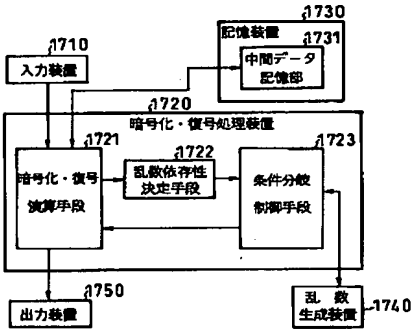
【図15】



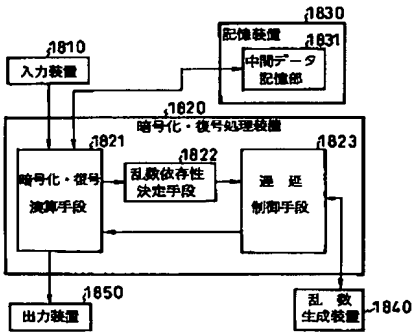
【図16】



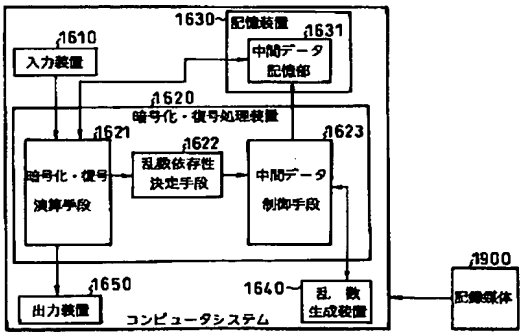
【図17】



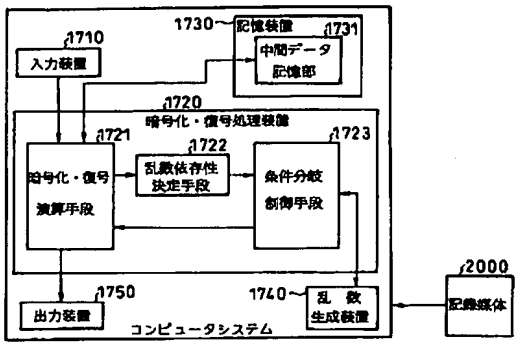
【図18】



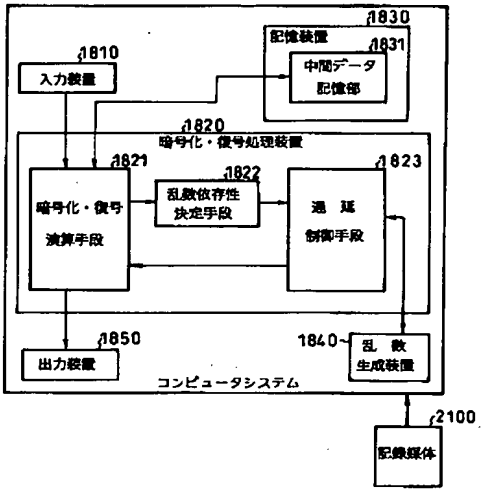
【図19】



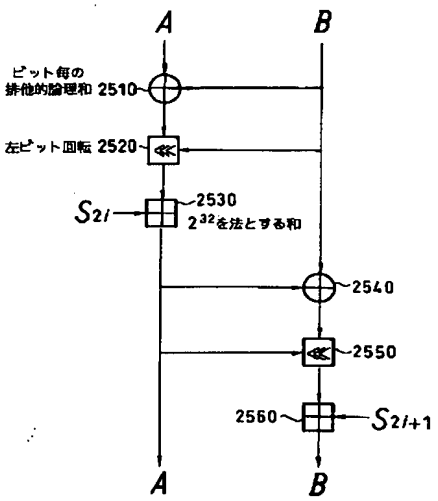
【図20】


1730
記憶装置
1731
中間データ記憶部
1710
入力装置
1720
暗号化・復号処理装置
1721
暗号化・復号演算手段
1722
乱数依存性決定手段
1723
条件分岐制御手段
1750
出力装置
1740
乱数生成装置
コンピュータシステム
2000
記録媒体

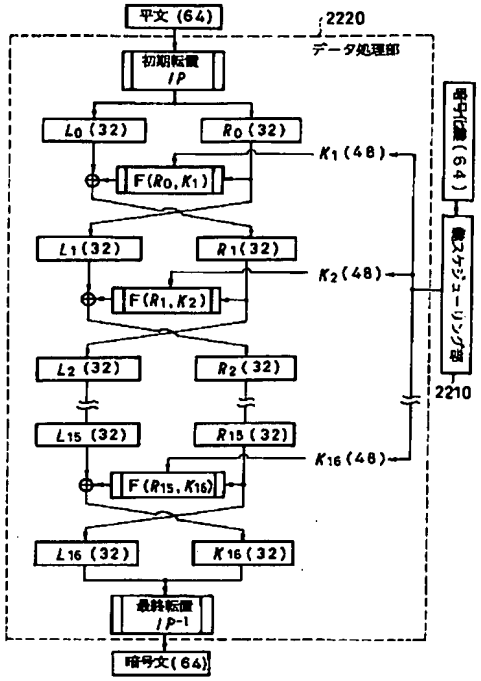
【図21】


1830
記憶装置
1831
中間データ記憶部
1810
入力装置
1820
暗号化・復号処理装置
1821
暗号化・復号演算手段
1822
乱数依存性決定手段
1823
遅延制御手段
1850
出力装置
1840
乱数生成装置
コンピュータシステム
2100
記録媒体

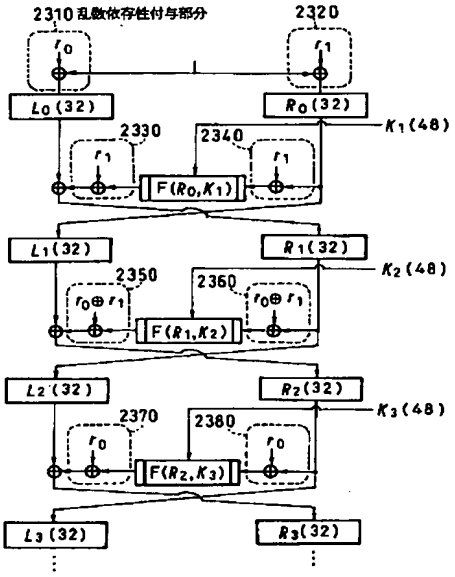
【図25】


A
B
ビット毎の排他的論理和 2510
左ビット回転 2520
S2i
2530
2^32を法とする和
2540
2550
2560
S2i+1
A
B

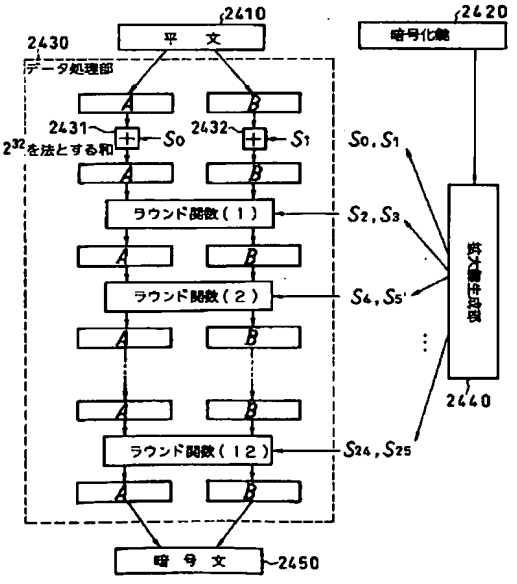
【図22】


平文(64)
2220
データ処理部
初期転置 IP
L_0(32)
R_0(32)
K_1(48)
$F(R_0, K_1)$
L_1(32)
R_1(32)
K_2(48)
$F(R_1, K_2)$
L_2(32)
R_2(32)
L_{15}(32)
R_{15}(32)
K_{16}(48)
$F(R_{15}, K_{16})$
L_{16}(32)
R_{16}(32)
最終転置 IP^{-1}
暗号文(64)
鍵中化部(64)
鍵スケジューリング部
2210

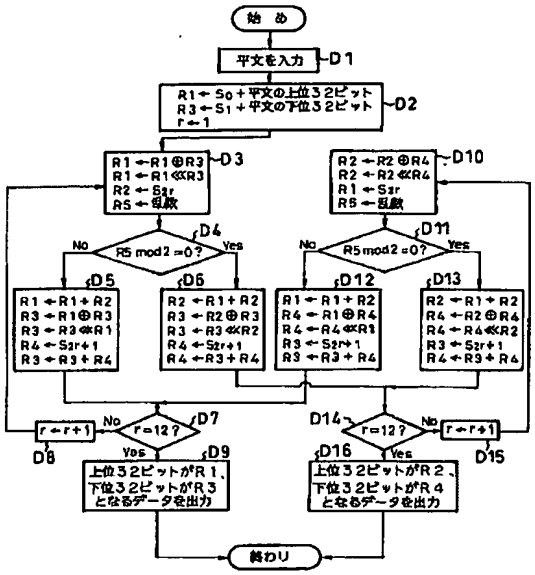
【図23】


2310 乱数依存性付与部分
2320
r_0
r_1
L_0(32)
R_0(32)
K_1(48)
2330
2340
$F(R_0, K_1)$
L_1(32)
R_1(32)
K_2(48)
2350
2360
$r_0 \oplus r_1$
$F(R_1, K_2)$
L_2(32)
R_2(32)
K_3(48)
2370
2380
$F(R_2, K_3)$
L_3(32)
R_3(32)

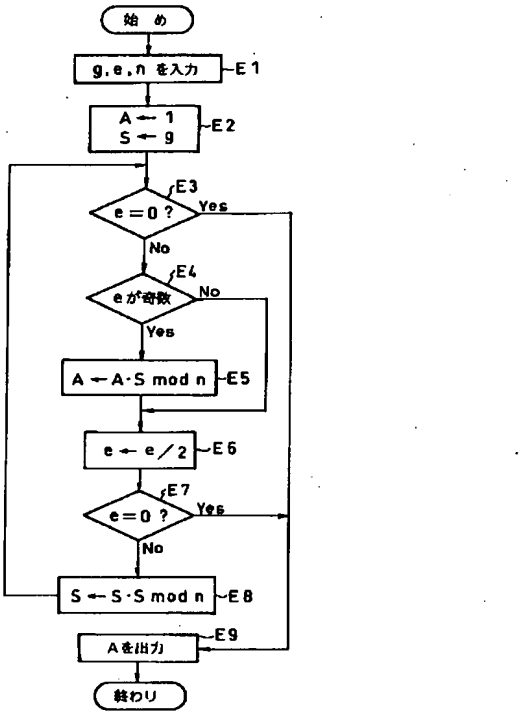
【図24】


2410
平 文
2420
暗号化鍵
2430
データ処理部
2431
2432
2^{32}を法とする和
S_0
S_1
S_0, S_1
ラウンド関数(1)
S_2, S_3
ラウンド関数(2)
S_4, S_5
ラウンド関数(12)
S_{24}, S_{25}
拡大鍵生成部
2440
暗 号 文
2450

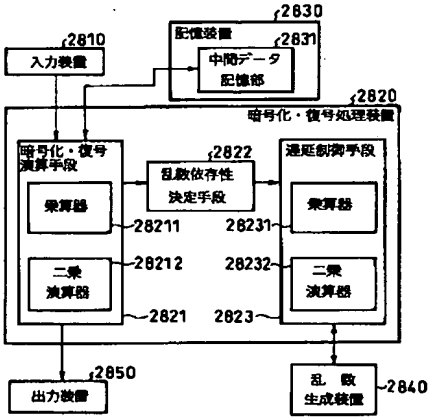
【図26】


始め
平文を入力
D1
R1←S0+平文の上位32ビット
R3←S1+平文の下位32ビット
r←1
D2
R1←R1⊕R3
R1←R1≪R3
R2←Sr
R5←乱数
D3
R2←R2⊕R4
R2←R2≪R4
R1←Sr
R5←乱数
D10
D4
R5 mod2 =0?
No
Yes
D11
R5 mod2 ≠0?
D5
R1←R1+R2
R3←R1⊕R3
R3←R3≪R1
R4←Sr+1
R3←R3+R4
D6
R2←R1+R2
R3←R2⊕R3
R3←R3≪R2
R4←Sr+1
R4←R3+R4
D12
R1←R1+R2
R4←R1⊕R4
R4←R4≪R1
R3←Sr+1
R3←R3+R4
D13
R2←R1+R2
R4←R2⊕R4
R4←R4≪R2
R3←Sr+1
R4←R3+R4
r←r+1
D8
r=12?
D7
D14
r=12?
r←r+1
D15
D9
上位32ビットがR1、
下位32ビットがR3
となるデータを出力
D16
上位32ビットがR2、
下位32ビットがR4
となるデータを出力
終わり

【図27】


始め
g,e,n を入力
E1
A←1
S←g
E2
E3
e=0?
Yes
No
E4
eが奇数
No
Yes
A←A·S mod n
E5
e←e/2
E6
E7
e=0?
Yes
No
S←S·S mod n
E8
Aを出力
E9
終わり

【図28】


2830
記憶装置
2810
入力装置
2831
中間データ
記憶部
2820
暗号化・復号処理装置
暗号化・復号
演算手段
2822
乱数依存性
決定手段
遅延制御手段
乗算器
28211
28231
乗算器
二乗
演算器
28212
28232
二乗
演算器
2821
2823
2850
出力装置
乱 数
生成装置
2840